

**Faculté des sciences économiques,
sociales, politiques et de communication**

Gouvernance belge du numérique et compliance : le cas de la directive européenne NIS

Auteur : GÜNAYDIN Erdem
Promoteur(s) : PRADELLA Sébastien
Année académique 2022-2023
Intitulé du master et de la finalité : Master 120 en Sciences politiques,
orientation générale (HD)

Remerciements

J'aimerais avant toute chose pouvoir témoigner de ma gratitude envers les personnes qui m'ont permises de réaliser ce mémoire.

Tout d'abord, je tiens à fortement remercier Monsieur Sébastien Pradella, qui m'a fourni un encadrement exceptionnel tout au long de ce processus de rédaction.

Je tiens également à remercier tout le corps professoral de l'UCLouvain FUCaM Mons. Au cours de ces dernières années, nous avons pu avoir la chance de suivre les cours de professeurs passionnés par leurs matières enseignées qui ont réussi à nous transmettre cette passion. De plus, je ne voudrais également pas oublier de citer les services administratifs de notre faculté qui ont toujours su répondre à chacune de nos inquiétudes et problèmes divers avec la plus grande des bienveillances.

Enfin, je tiens à remercier mes camarades de classe ainsi que ma famille pour leur soutien infaillible pendant chaque moment difficile de ces dernières années.

Table des matières

Table des abréviations	5
Liste des illustrations.....	6
Liste des tableaux	7
Liste des annexes.....	8
Chapitre 1 : Introduction	9
A. Introduction générale	9
1. La cybersécurité en Europe.....	9
2. La cybersécurité en Belgique.....	12
3. La directive Network and Information Systems (NIS)	15
B. Méthodologie.....	23
1. Problématique de la recherche	23
2. Justification du choix du terrain.....	23
3. Modèle d'analyse	25
4. Collecte de données	25
C. Hypothèse	26
Chapitre 2 : Etat de l'art	27
A. Analyse de la directive NIS	27
1. Exigences de la directive.....	27
2. Processus d'adoption	29
B. La « <i>compliance</i> » en politiques publiques	31
C. « Why non-compliance ».....	44
1. Introduction.....	44
2. Le modèle « PCP » (Pouvoir, Capacité et Politisation)	45
D. La transposition de politiques publiques	49
Chapitre 3 : Les processus de « <i>taking</i> » et de « <i>shaping</i> » par la Belgique dans le cadre de la directive NIS	56
A. Présentation du contexte	56
B. Le processus de « <i>taking</i> ».....	58
1. Les ressources	59
2. L'efficacité bureaucratique	63
3. L'autonomie domestique	66
4. Résultats.....	67
C. Processus de « <i>shaping</i> » (façonnage).....	69
1. Le niveau « domestique »	69
2. Le niveau européen	70
3. Résultats.....	71

D.	Conclusions	72
E.	Discussion et limites de la recherche.....	75
Bibliographie		77

Table des abréviations

OSE : Opérateurs de services essentiels

FSN : Fournisseurs de services numériques

Directive NIS : Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

ANSSI : Agence nationale de la sécurité des systèmes d'information

CCB : Centre pour la Cybersécurité de Belgique

CIRT : Computer emergency response team

ISAC : Information Sharing and Analysis Center

Liste des illustrations

Figure 1: Acteurs européens de la cybersécurité.....	12
Figure 2: Récapitulatif des exigences de la Directive NIS.....	17
Figure 3: modélisation du modèle PCP	25
Figure 4: Résumé du processus législatif de la directive NIS 1	30
Figure 5 : Récapitulatif des acteurs concernés par la directive NIS.....	58

Liste des tableaux

Tableau 1 : Adapté de "Three worlds of compliance" (Falkner, Hartlapp & Treib, 2007).....	35
Tableau 2 : Adapté de "PCP in a two-level compliance game across two stages" (Börzel, 2021).....	47

Liste des annexes

- 1) Enregistrements et retranscriptions des entretiens effectués (**disponible sur demande**)

Chapitre 1 : Introduction

A. Introduction générale

1. La cybersécurité en Europe

i. *Historique*

L'Union européenne s'est emparée de la question de la cybersécurité dès le XXI^e siècle, avec la montée en puissance d'Internet et des technologies de l'information. Les Etats membres de l'Union ont commencé dès lors à prendre conscience des défis et des menaces liés à la cybersécurité. Les premiers incidents et attaques cyber ont mis en évidence la nécessité de renforcer la sécurité des systèmes d'information.

Conscient de cette menace grandissante sur l'ensemble de ses systèmes d'information l'Union a décidé en 2004, de créer l'Agence de l'Union européenne pour la cybersécurité (ENISA) afin de renforcer la coopération et l'expertise en matière de cybersécurité. L'ENISA a pour mission de soutenir les États membres de l'UE dans la mise en œuvre de mesures de cybersécurité efficaces, de favoriser la sensibilisation et de coordonner les activités de réponse aux incidents.

Néanmoins, désireuse de vouloir mettre en place une gouvernance harmonisée de cybersécurité, l'Union européenne a décidé d'adopter sa première stratégie européenne de cybersécurité en 2013. Cette stratégie avait pour but de renforcer la résilience de l'UE face aux cybermenaces et à promouvoir une approche globale de la cybersécurité, en mettant l'accent sur la prévention, la détection, la réaction et la coopération internationale. Nous étions dès lors dans les premières phases de la gouvernance européenne de la question de la cybersécurité.

En 2016, l'Union européenne a adopté sa directive sur la sécurité des réseaux et des systèmes d'information (NIS). Cette directive établit un cadre de cybersécurité harmonisé au niveau de l'UE, en imposant des obligations aux opérateurs de services essentiels et aux fournisseurs de services numériques en matière de sécurité des réseaux et des systèmes d'information (voir infra) dans une volonté de protéger les services essentiels des Etats membres. La directive impose des niveaux de sécurité afin de diminuer les risques d'indisponibilité de service des entités essentielles (telle que la distribution d'eau, la santé, les finances, etc.) Cette directive encourage également la coopération entre les États membres et la notification des incidents de sécurité.

L'Union européenne a depuis renforcé la coopération et la coordination en matière de cybersécurité. Des initiatives ont été lancées pour promouvoir l'échange d'informations, la coordination des actions et la collaboration entre les États membres, les institutions européennes, les organismes de cybersécurité et le secteur privé. A titre d'exemple, beaucoup de partenaires du secteur public se réunissent dans des conférences internationales sur le sujet à des intervalles réguliers.

En 2019, l'Union européenne a adopté une nouvelle stratégie de cybersécurité (« Cyber Security Act »), qui vise à renforcer la résilience de l'Union face aux cybermenaces. La stratégie met l'accent sur cinq piliers : la résilience, la dissuasion, la détection, la réaction et la coopération internationale. Elle souligne également la nécessité d'investir dans la recherche et l'innovation en matière de cybersécurité. Ce point est également un point clé des stratégies nationales cyber des États membres.

Sur le plan légal, l'Union européenne a également renforcé son cadre juridique en matière de cybersécurité. En plus de la directive NIS, le Règlement général sur la protection des données (« RGPD ») et d'autres réglementations ont été adoptés pour garantir la protection des données personnelles et renforcer la sécurité des systèmes d'information au sein de l'UE.

L'Union européenne a donc progressivement renforcé sa gouvernance de la cybersécurité au fil des années. De la création de l'ENISA à l'adoption de stratégies et de réglementations spécifiques, l'UE vise à renforcer la résilience de ses États membres face aux cybermenaces, à promouvoir la coopération et la coordination, ainsi qu'à protéger les données personnelles et les infrastructures numériques critiques.

ii. Instruments

Afin de garantir la cybersécurité, l'Union européenne a dû se munir de plusieurs instruments et initiatives en matière de cybersécurité pour renforcer la sécurité des systèmes d'information et protéger les infrastructures numériques. Celles-ci sont par exemple (*Cybersécurité: comment l'UE lutte contre les cybermenaces*, 2023) :

- Directive NIS
- Stratégie de cybersécurité de l'UE
- CERT-EU : Le CERT-EU est l'équipe d'intervention d'urgence informatique de l'UE, chargée de gérer les incidents de sécurité informatique au sein des institutions de l'UE. Il fournit une assistance technique, des conseils et des recommandations en cas d'incident de cybersécurité aux États membres.

- Programmes de financement et de recherche : L'UE soutient la cybersécurité à travers différents programmes de financement et de recherche, tels que le programme de recherche et d'innovation Horizon 2020 et le programme de financement de la cybersécurité de l'UE. Ces programmes encouragent la collaboration, le développement de technologies de pointe et l'échange de connaissances dans le domaine de la cybersécurité.
- Coopération internationale : L'Union européenne développe des partenariats et des mécanismes de coopération avec des pays tiers et des organisations internationales pour promouvoir la cybersécurité à l'échelle mondiale. Elle participe également à des initiatives multilatérales visant à renforcer la stabilité et la sécurité dans le cyberspace (notamment via le groupe de coopération NIS).

Pour garantir une coopération internationale efficace, l'Union européenne a mis au point les « ISAC ». Les ISAC (Information Sharing and Analysis Centers) sont des organisations ou des consortiums qui facilitent l'échange d'informations sur les menaces, les vulnérabilités et les incidents de cybersécurité entre les entités publiques et privées d'un secteur spécifique. Ils jouent un rôle essentiel dans l'amélioration de la posture de cybersécurité et la résilience des infrastructures critiques et des industries sensibles.

En Europe, les ISAC fonctionnent selon des modèles et des structures différents dans chaque pays. Cependant, leur objectif principal est de promouvoir la collaboration et l'échange d'informations entre les acteurs du secteur concerné, afin de renforcer la capacité collective à faire face aux cybermenaces. (*Information Sharing and Analysis Centers (ISACs)*, s. d.)

Les ISAC rassemblent des organisations du secteur public et privé, telles que des entreprises, des organismes gouvernementaux, des opérateurs d'infrastructures critiques, des fournisseurs de services de sécurité, des universités et des centres de recherche. Ils collectent et analysent des informations sur les incidents de cybersécurité, les techniques d'attaque, les vulnérabilités et les meilleures pratiques de protection. Ces informations sont ensuite partagées avec les membres de l'ISAC, ce qui permet une meilleure compréhension des menaces émergentes, une réponse plus rapide aux incidents et une amélioration de la prévention et de la protection des systèmes d'information. Les ISAC ont également pour mission de sensibiliser les acteurs du secteur concerné aux risques de cybersécurité, d'organiser des formations et des exercices de simulation, de développer des recommandations et des normes de sécurité, et de coordonner la collaboration avec les autorités gouvernementales et les organismes chargés de la sécurité nationale. (*Information Sharing and Analysis Centers (ISACs)*, s. d.)

Les ISAC jouent dès lors un rôle crucial dans la promotion de la confiance, de la collaboration et de la résilience au sein des secteurs et des industries exposés aux cybermenaces. Ils contribuent à l'amélioration de la posture de cybersécurité en favorisant le partage d'informations, la coordination des réponses aux incidents et l'adoption de bonnes pratiques de sécurité. (*Empowering EU-ISACs*, s. d.).

En outre, l'Europe a également créé un groupe de coopération NIS. Ce groupe est soutenu par des travaux les différentes équipes d'interventions d'incidents de sécurité (CSIRT). (*Groupe de coopération SRI*, s. d.).

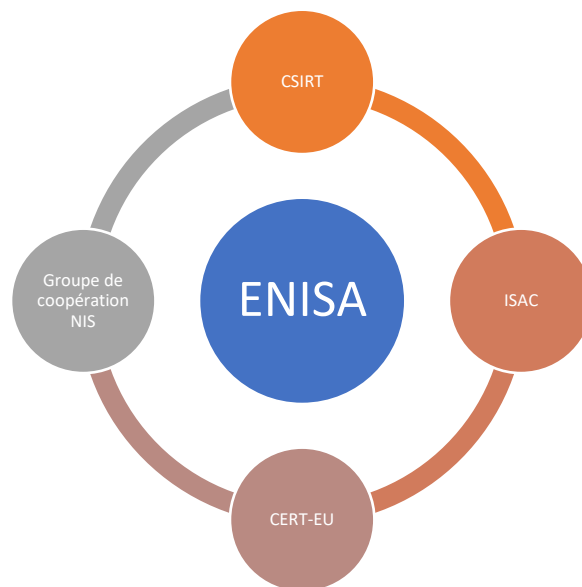


Figure 1: Acteurs européens de la cybersécurité

Ces instruments de l'Union européenne visent à renforcer la résilience de l'UE face aux cybermenaces, à promouvoir la coopération entre les États membres, les institutions de l'UE et les acteurs privés, et à garantir la protection des infrastructures et des services numériques essentiels pour l'ensemble de l'Union européenne.

2. La cybersécurité en Belgique

i. *Historique*

En Belgique, la gestion de la question de la cybersécurité a été différente de ce qu'on a pu connaître sur le plan européen.

Au début des années 2000, la Belgique a commencé à prendre conscience des enjeux liés à la cybersécurité. Avec la croissance rapide de l'utilisation d'Internet et des technologies

numériques, il est devenu évident que des mesures spécifiques étaient nécessaires pour protéger les infrastructures critiques et les données sensibles contre les cybermenaces.

Afin d'avoir un organe compétent en la matière, le gouvernement belge a créé le Centre de Cybersécurité Belge (CCB) en 2014 en tant qu'organe national de coordination de la cybersécurité. Placé sous l'autorité du Premier Ministre, le CCB est chargé de la coordination des politiques et des actions relatives à la cybersécurité. Il collabore avec les acteurs publics et privés pour renforcer la sécurité des réseaux et des systèmes d'information du pays. (CCB - *Organisation*, 2023)

Le CCB est donc l'acteur principal de la stratégie cyber belge, qui a vu le jour en 2012 et a été mise à jour en 2016 pour couvrir la période 2016-2020. Cette stratégie a établi une feuille de route pour renforcer la cybersécurité en Belgique. Elle comprend trois axes principaux : la protection des infrastructures critiques, la sensibilisation à la cybersécurité et le renforcement des capacités (*Stratégie cybersécurité Belgique*, 2021).

- La stratégie mettait l'accent sur la protection des infrastructures essentielles, telles que les réseaux électriques, les services financiers, les réseaux de communication et les services de santé. Des mesures ont été mises en place pour évaluer les risques, renforcer la résilience des systèmes et promouvoir les bonnes pratiques de sécurité.
- La stratégie visait à accroître la sensibilisation à la cybersécurité dans la société belge. Des campagnes de sensibilisation ont été lancées pour informer et éduquer les citoyens, les entreprises et les organisations sur les risques liés à la cybersécurité, ainsi que sur les mesures de protection appropriées.
- La stratégie reconnaissait l'importance du renforcement des compétences en matière de cybersécurité. Des initiatives ont été prises pour améliorer la formation et le développement des compétences des professionnels de la cybersécurité. Des programmes de formation, de certification et de sensibilisation ont été mis en place pour améliorer les connaissances et les compétences dans ce domaine.

En 2018, la Belgique a adopté une loi sur la sécurité des réseaux et des systèmes d'information pour transposer la directive européenne NIS dans la législation belge. Cette loi impose des obligations de sécurité aux opérateurs de services essentiels et aux fournisseurs de services numériques. Ce point sera détaillé dans le chapitre consacré à la directive.

ii. Stratégie

La Belgique s'est dotée d'une stratégie de cybersécurité en 2012.

Ce plan d'action national vise à renforcer la cybersécurité en Belgique et à protéger les infrastructures critiques, promouvoir la sensibilisation à la cybersécurité et renforcer les capacités de lutte contre les cyberattaques. (*ECS – DigitalEurope*, 2019).

La stratégie belge de cybersécurité est donc un plan d'action complet visant à renforcer la sécurité numérique en Belgique en mettant l'accent sur la protection des infrastructures critiques, la sensibilisation à la cybersécurité.

La stratégie de cybersécurité 2.0 de 2021 est la mise à jour et l'évolution de la Stratégie belge de cybersécurité 2012-2020. Il existe plusieurs différences entre les stratégies (*Une cyberstratégie 2.0 pour propulser la Belgique au rang des pays les moins vulnérables d'Europe*, 2021) :

- La stratégie de cybersécurité 2.0 adopte une approche plus large et englobe les enjeux actuels et futurs de la cybersécurité. Elle tient compte des nouvelles technologies émergentes, telles que l'Internet des objets (IoT), l'intelligence artificielle (IA) et le cloud computing, ainsi que des nouvelles menaces et vulnérabilités qui en découlent.
- La stratégie de cybersécurité 2.0 établit de nouveaux objectifs et priorités en matière de cybersécurité. Elle met davantage l'accent sur la protection des données personnelles, la résilience des infrastructures numériques, la lutte contre la cybercriminalité, la promotion de l'innovation et le renforcement de la coopération internationale.
- La stratégie de cybersécurité 2.0 reconnaît l'importance du renforcement des capacités en matière de cybersécurité. Elle met l'accent sur la formation, le développement des compétences et la sensibilisation à la cybersécurité à tous les niveaux de la société belge, notamment en encourageant la formation spécialisée, la recherche et le développement des talents dans le domaine de la cybersécurité.
- La stratégie de cybersécurité 2.0 souligne l'importance de la collaboration et de la coordination entre les acteurs publics et privés. Elle encourage le partage d'informations, la coopération opérationnelle et l'échange de bonnes pratiques entre les différents acteurs impliqués dans la cybersécurité, y compris les organismes gouvernementaux, les entreprises, les institutions académiques et les organisations de la société civile.
- La stratégie de cybersécurité 2.0 met l'accent sur le renforcement du cadre juridique en matière de cybersécurité. Elle vise à adapter et à renforcer la législation existante pour répondre aux défis émergents, tels que la protection des données, la cybercriminalité et la protection des infrastructures numériques critiques.

La stratégie de cybersécurité 2.0 de 2021 élargit la portée et les objectifs de la Stratégie belge de cybersécurité 2012-2020 pour tenir compte des évolutions technologiques et des nouvelles menaces. Elle met l'accent sur la protection des données, la résilience des infrastructures numériques, la coopération et le renforcement des capacités en matière de cybersécurité.

D'une part, les avancées technologiques telles que l'Internet des objets (« IoT »), l'intelligence artificielle (IA), le cloud computing et la 5G ont considérablement transformé la manière dont nous interagissons avec les systèmes d'information. Ces nouvelles technologies créent de nouveaux défis en matière de cybersécurité, notamment en termes de vulnérabilités et de vecteurs d'attaque.

Les cybermenaces évoluent et se sophistiquent constamment. Les attaques informatiques deviennent plus complexes, ciblées et coordonnées. Les cybercriminels et les acteurs étatiques malveillants sont de plus en plus compétents et organisés. Les menaces telles que les attaques par ransomware, l'espionnage industriel, le vol de données sensibles et la manipulation de l'opinion publique nécessitent des approches adaptées.

Au fil des années, la sensibilisation à la cybersécurité s'est accrue. Les incidents de sécurité médiatisés, les fuites de données massives et les perturbations majeures causées par des attaques ont mis en évidence l'importance critique de la cybersécurité pour la stabilité économique, la sécurité nationale et la vie quotidienne des citoyens. Une stratégie 2.0 permet de répondre aux attentes croissantes en matière de protection des informations et de garantie de la confiance numérique.

Les stratégies de cybersécurité doivent donc évoluer pour s'adapter aux nouvelles réalités et aux enjeux émergents. Les politiques et les approches développées dans la première stratégie peuvent devenir obsolètes face à la rapidité des évolutions technologiques et des menaces. Une stratégie 2.0 offre l'opportunité de réévaluer les priorités, de mettre à jour les mesures de sécurité, de renforcer les capacités et de promouvoir l'innovation.

3. La directive Network and Information Systems (NIS)

i. Introduction

La Directive NIS (Network and Information Security) est une directive européenne adoptée par l'Union européenne en 2016 et qui vise à renforcer la cybersécurité au sein de l'UE. Elle est également connue sous le nom de directive 2016/1148 ou directive sur la sécurité des réseaux et des systèmes d'information (NIS). (Mathias, 2018)

L'objectif principal de la directive NIS est d'améliorer la sécurité des infrastructures critiques et des services numériques essentiels au sein de l'UE. Ces infrastructures et services incluent des secteurs tels que l'énergie, les transports, la santé, les services bancaires, les services en ligne, les opérateurs de services essentiels (OSE) et les fournisseurs de services numériques (FSN). La directive vise à garantir la disponibilité, l'intégrité, la résilience et la sécurité de ces infrastructures et services.

Les États membres sont tenus d'identifier les opérateurs de services essentiels (OSE) et les fournisseurs de services numériques (« FSN », tels que les prestataires de cloud, moteurs de recherche, etc.) relevant de la directive. Les critères d'identification comprennent l'impact qu'une panne de service pourrait avoir sur la société, l'économie et la sécurité nationale.

Les OSE et les FSN identifiés doivent prendre des mesures de sécurité appropriées pour gérer les risques de cybersécurité et assurer un niveau élevé de sécurité de leurs réseaux et systèmes d'information. Ils doivent mettre en place des mesures de sécurité proportionnées à leurs risques spécifiques, telles que la prévention des incidents, la gestion des incidents, la surveillance, la détection et la réponse aux incidents de cybersécurité.

La directive encourage également la coopération entre les États membres et les acteurs concernés, tels que les OSE, les FSN et les autorités nationales compétentes en matière de cybersécurité. Les États membres doivent établir des mécanismes de coopération, des points de contact (notamment via les ISAC) et des réseaux d'alerte pour faciliter l'échange d'informations sur les incidents de cybersécurité et les meilleures pratiques dans le domaine.

Les OSE et les FSN doivent notifier les incidents de sécurité ayant un réel impact sur la disponibilité de leurs services aux autorités nationales compétentes en matière de cybersécurité.

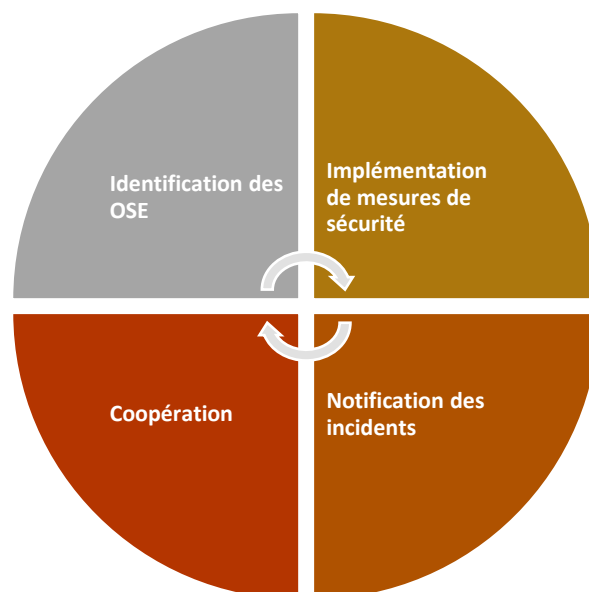


Figure 2: Récapitulatif des exigences de la Directive NIS

Les États membres sont tenus de mettre en place des procédures pour la notification des incidents, la gestion des crises et la coopération en cas d'incident transfrontalier.

De plus, chaque État membre est tenu de désigner une ou plusieurs autorités nationales compétentes en matière de cybersécurité pour superviser la mise en œuvre de la directive sur leur territoire. Ces autorités sont chargées de veiller à la conformité des OSE et des FSN, de faciliter la coopération et l'échange d'informations, et de coordonner les actions en cas d'incident de cybersécurité. En Belgique, comme mentionné plus haut, cette autorité est le CCB.

Des sanctions sont également prévues si des incidents ne sont pas signalés à ces autorités nationales.

La directive impose donc un cadre réglementaire commun pour la cybersécurité dans l'Union et renforce la coopération entre les États membres pour faire face aux cybermenaces et aux incidents de cybersécurité. Elle contribue à créer un environnement plus sûr pour les infrastructures et les services numériques essentiels, renforçant ainsi la confiance des citoyens, des entreprises et des administrations dans l'utilisation des technologies numériques.

Il convient de noter que la directive NIS a été transposée dans les législations nationales des États membres, ce qui peut entraîner des différences dans la manière dont elle est mise en œuvre et appliquée dans chaque pays.

ii. Transposition de la directive

La transposition de la directive fera l'objet d'une analyse plus poussée dans ce mémoire, néanmoins, en guise d'introduction, il est important de dresser un premier bilan de celle-ci.

Pays pionniers dans la transposition :

Certains pays européens ont été rapides dans la transposition de la directive NIS. Nous citerons par exemple l'Estonie qui est considérée comme l'un des leaders de la cybersécurité en Europe. Le pays a adopté rapidement une loi de transposition de la directive NIS et a mis en place un cadre solide pour la protection des infrastructures critiques et des systèmes d'information. (*ANSIP : Estonia isn't perfect enough to teach other countries tech - The European Association of State Territorial Representatives*, s. d.).

Nous pouvons également citer l'Allemagne grâce à sa proactivité dans la transposition de la directive NIS. Le pays a adopté une loi nationale sur la cybersécurité en 2017 et a créé une autorité de cybersécurité dédiée chargée de la supervision et de la mise en œuvre de la directive. (*NIS Directive In Germany - Implementation & Specificities*, 2021).

Pays ayant transposé la directive avec des retards :

Certains pays européens ont pris plus de temps pour transposer la directive NIS. Nous citerons ici le cas de la Belgique qui a connu des retards dans la transposition de la directive NIS. La loi belge de transposition a été adoptée en 2019, soit quelques années après l'échéance initiale de la directive. Les défis liés à la coordination entre les différents niveaux de gouvernement ont été cités comme une des raisons du retard. (*3e anniversaire de la Loi nationale transposant la « Directive NIS »*, 2022). Ce point fera l'objet de l'analyse de ce mémoire.

Pays ayant rencontré des difficultés dans la transposition :

Certains pays européens ont rencontré des difficultés majeures dans la transposition de la directive NIS. La Grèce a connu des problèmes importants dans la transposition de la directive NIS. Des retards significatifs ont été observés et le pays a été mis en demeure par la Commission européenne pour non-transposition de la directive. La situation a depuis été rectifiée. (Maglaras et al., 2018). La Roumanie a également rencontré des difficultés dans la transposition de la directive NIS. Des retards importants ont été observés, notamment en raison de l'instabilité politique et des changements de gouvernement. Cependant, la Roumanie a finalement adopté une loi de transposition en 2019. (*Implementing the EU's NIS directive in Romania*, s. d.).

Les raisons dans le retard dans la transposition de la Directive NIS en Belgique étant le plus intéressants aux fins de ce mémoire, celles-ci seront étudiées dans le chapitre qui y est consacré.

Le tableau suivant récapitule l'état de la gestion de la question de la cybersécurité en Europe (*NIS Directive Tool*, s. d.) :

Pays	Date de la dernière stratégie cyber nationale	Transposition de la Directive NIS	Objectifs de la stratégie cyber	Autorité nationale ?
Allemagne	09/09/2021	Oui	9 objectifs	Office fédéral de la sécurité des technologies de l'information (BSI)
Autriche	22/12/2021	Oui	12 objectifs	Agence autrichienne de cybersécurité (AGES)
Belgique	20/05/2021	Oui	11 objectifs	Centre pour la Cybersécurité Belgique (CCB)
Bulgarie	18/07/2016	Oui	8 objectifs	Agence nationale de sécurité des systèmes d'information (SANS)
Chypre	03/12/2020	Oui	20 objectifs	Centre national de cybersécurité (NCSC-CY)
Croatie	07/10/2015	Oui	7 objectifs	Agence de sécurité de l'information (ISA)
Danemark	01/12/2021	Oui	11 objectifs	Centre d'alerte national danois pour la cybersécurité (DKCERT)
Espagne	01/04/2019	Oui	15 objectifs	Institut national de la cybersécurité (INCIBE)
Estonie	05/09/2019	Oui	17 objectifs	Agence de la sécurité des technologies de l'information (RIA)
Finlande	24/01/2013	Oui	14 objectifs	Centre national des opérations de cybersécurité (NCSC-FI)
France	10/10/2015	Oui	13 objectifs	Agence nationale de la sécurité des systèmes d'information (ANSSI)
Grèce	07/12/2020	Oui	20 objectifs	Organisation de la cybersécurité (OCS)

Hongrie	21/03/2018	Oui	9 objectifs	Centre hongrois de réponse aux incidents informatiques (CERT-Hungary)
Irlande	27/12/2019	Oui	19 objectifs	Centre national de cybersécurité (NCSC)
Italie	17/05/2022	Oui	21 objectifs	Agence nationale pour la cybersécurité (ANCS)
Lettonie	17/09/2019	Oui	9 objectifs	Centre de réponse aux incidents informatiques de Lettonie (CERT.LV)
Lituanie	13/08/2018	Oui	14 objectifs	Centre de réponse aux incidents informatiques de Lituanie (CERT-LT)
Luxembourg	11/10/2021	Oui	12 objectifs	Agence nationale de la sécurité des systèmes d'information (ANSSI-LU)
Malte	26/09/2016	Oui	6 objectifs	Agence de sécurité des systèmes d'information de Malte (MISA)
Norvège	31/01/2019	Oui	15 objectifs	Centre national de cybersécurité (NorCERT)
Pays-Bas	21/04/2018	Oui	7 objectifs	Centre national pour la sécurité des systèmes d'information (NCSC)
Pologne	31/10/2019	Oui	13 objectifs	Centre de sécurité informatique national (NASK-CERT)
Portugal	06/06/2019	Oui	12 objectifs	Centre national de cybersécurité (CNCS)
République tchèque	18/03/2021	Oui	19 objectifs	Centre de réponse aux incidents informatiques (CSIRT.CZ)
Roumanie	30/12/2021	Oui	20 objectifs	Agence nationale de sécurité des systèmes d'information (ANSSI)
Royaume-Uni	29/11/2016	Oui	12 objectifs	Centre de réponse aux incidents informatiques de Roumanie (CERT-RO)
Slovaquie	07/01/2021	Oui	20 objectifs	Centre de réponse aux incidents informatiques de Slovaquie (SK-CERT)
Slovénie	01/02/2016	Oui	10 objectifs	Centre national de cybersécurité (NCSC-SI)

Suède	22/06/2017	Oui	10 objectifs	Agence suédoise pour la cybersécurité (MSB)
Suisse	18/04/2018	Oui	13 objectifs	Centre national suisse pour la cybersécurité (NCSC)

iii. La nécessité d'avoir une deuxième version de la Directive

La commission Européenne a décidé de mettre à jour sa directive Network and Information Systems (NIS) en décembre 2020. Celle-ci a été adoptée en novembre 2022.

La nécessité de la mise à jour s'est fait ressentir après les premiers retours sur la directive NIS1. En effet, le champ d'application de la directive n'était pas assez large. De nouveaux secteurs ont été introduits dans la directive ainsi que des subdivisions au sein même de ces secteurs. A titre d'exemple, le secteur de la santé ne se limite plus uniquement aux hôpitaux mais également aux laboratoires, fournisseurs de matériel médical ou pharmaceutique, etc.

En outre, la directive NIS2 introduit de nouveaux concepts. Par exemple, l'identification n'est plus un critère pour tomber sous le champ d'application de la directive (le fait d'avoir 50 employés ou plus et d'avoir un chiffre d'affaires de minimum 10 millions d'euros fait tomber de facto sous le champ d'application de celle-ci).

La distinction entre Opérateurs de services essentiels et Fournisseurs de services digitaux disparaît également pour laisser place à deux nouvelles catégories : les entités hautement critiques et critiques.

La première vise les grandes entreprises se trouvant dans les secteurs repris à l'annexe 1 de la directive (voir tableau infra) avec 250 employés ou avec un chiffre d'affaires égal à 50 millions d'euros par an.

La deuxième vise les moyennes entreprises des secteurs repris dans les catégories des annexes de la directive avec au minimum 50 employés et moins de 50 millions d'euros de chiffres d'affaires annuel. Néanmoins, certaines entreprise (même si elle ne répondent pas aux critères minimums des entités importantes) sont de facto classées parmi les entités essentielles (exemple : les fournisseurs de réseaux de communications électroniques publiques). (*The NIS 2 Directive : What does it mean for my organization ?*, 2023)

Le tableau suivant donne une indication quant aux nouveaux secteurs de la directive NIS2 comparés à la directive NIS 1 (*EUR-LEX - 32022L2555 - EN- EUR-LEX*, s. d.) :

NIS 2	NIS 1
Secteurs hautement critiques	Opérateurs de services essentiels
Energie	Energie
Transport	Transport
Banques	Finances
Infrastructures financières	
Santé	Santé
Eau	Eau potable
Infrastructures digitales	Infrastructures numériques
Services TIC	
Administration publiques	Inexistant
Espace	
Secteurs critiques	/
Services postaux	/
Gestion des déchets	
Fabrication, production et distribution des produits chimiques	
Fabrication, production et distribution des denrées alimentaires	
Fabrication	
Fournisseurs numériques	
Recherche	

Néanmoins, ce mémoire ne traitera pas directement de la directive NIS2 car celle-ci vient tout juste d'entrer en application. Comme sa précédente version, il y aura un délai pour la transposition de la directive dans les législations nationales. Etant dans une phase précoce pour le moment, cette réalité ne pourra être étudiée avec les données dont nous disposons actuellement.

B. Méthodologie

1. Problématique de la recherche

La cybersécurité est un sujet qui préoccupe de plus en plus les Etats. Les attaques se diversifient, les menaces se multiplient et les vulnérabilités ne font que croître. Dans un contexte tel que celui-ci, nous sommes en droit de nous demander comment les Etats protègent leurs citoyens face à ces menaces grandissantes.

Il est évident que chaque pays dispose d'une stratégie plus ou moins poussée selon les différents contextes mais est-ce que cette protection s'avère suffisante ou efficace ? Etant donné l'interconnexion qu'il existe au sein de l'Union entre les différents Etats membres, cette problématique est, de manière logique, traitée conjointement par ceux-ci.

Comme nous l'avons mentionné, la directive NIS1 semble être le sujet parfait pour pouvoir étudier cette volonté de pouvoir protéger les infrastructures critiques d'un Etat afin d'assurer aux citoyens un service continu. Néanmoins, après de courtes recherches sur le sujet, il apparaît que tous les pays ne sont pas au même niveau de maturité quant au respect des obligations de la directive NIS1, malgré qu'elle soit le fruit de travaux parlementaires communs et bien que celle-ci ait été votée à l'unanimité sans voix d'opposition.

Dès lors, nous sommes confrontés à une question importante. Comment les Etats, s'ils sont convaincus du bien-fondé d'une directive ayant un effet direct sur la gestion de la cybersécurité interne aux Etats membres, peuvent-ils tantôt afficher une conformité plus exemplaire alors que d'autres ne réalisent pas (ou ne sont pas en mesure) un constat identique ?

De ce fait, cette question nous a amené sur la problématique que nous essayerons de traiter dans ce mémoire :

« Comment pouvons-nous expliquer la « compliance » à la directive NIS 1 au sein de la Belgique ? »

2. Justification du choix du terrain

Ayant travaillé dans le secteur de la sécurité de l'information et ayant eu la chance de collaborer avec plusieurs entités du secteur privé et public, nous avons pu constater que cette directive laissait perplexe beaucoup de personnes concernées. Retard, incompréhension, frustrations, ... tout ceci indique qu'il existe potentiellement un malaise plus général concernant la conformité à cette directive. Afin de faire le lien avec l'objet de nos études, il paraissait intéressant d'analyser toutes ces raisons sur le plan des Sciences politiques.

Avant toute chose, il est important de préciser que ce mémoire n'a pas pour but de faire une étude comparative entre les pays de l'Union européenne. La raison principale est que cette étude ne peut faire l'objet d'un mémoire car l'analyse serait beaucoup trop longue et fastidieuse pour des résultats plus que suspects. En effet, il ne faut pas comparer la réalité d'un pays de manière aléatoire à un autre car les contextes qui les concernent peuvent être fondamentalement différents. La base de la limitation du choix du terrain s'inscrit également dans la continuité de nos apprentissages lors de ce Master. Nous avons pu voir lors de cours comme « Analyse et Evaluation de Politiques Publiques » qu'il existe des logiques de conformité différentes entre les pays européens qui peuvent être classifiés en trois mondes distincts (Falkner, Hartlapp & Treib, 2007). Ce point sera néanmoins détaillé plus bas.

Néanmoins, il reste que le sujet doit toujours être analysé de manière à pouvoir répondre à la problématique de manière efficace et surtout pertinente.

C'est pourquoi nous avons choisi d'étudier le cas de la Belgique pour cette mise en conformité. Cette analyse nous permettrait d'étudier la question en profondeur, de mobiliser les apprentissages de ces dernières années et de vérifier notre manière de réflexion par rapport à un sujet inhabituel comme la cybersécurité (souvent analysé d'un point de vue technique).

Nous avons pu identifier lors de nos recherches préliminaires que cette question était gérée de manière sectorielle en Belgique (ce qui correspond aux cinq secteurs minimums de la directive). Nous avons pu également voir que des problèmes se posaient dans la gestion de cette thématique dans le secteur de l'Eau (pas de comité sectoriel contrairement aux autres secteurs). C'est pourquoi nous avons choisi d'analyser ce secteur plus particulièrement et, afin de confronter nos résultats à un autre secteur, de travailler également en comparaison avec le secteur du Transport. En dehors de ces secteurs, il nous a paru comme étant essentiel d'avoir un avis de l'autorité compétente qui gère cette matière au niveau national. De plus, un point de vue d'un expert sur la question nous permettrait également d'obtenir des réponses que nous ne pourrions avoir d'autres types d'acteurs. C'est pourquoi nous avons également choisi d'interroger le professeur de l'Ecole Polytechnique de Louvain, Axel Legay, faisant également partie de la « Coalition Cybersécurité » qui est un partenariat entre le monde académique, le secteur privé et public (*Cyber Security Coalition*, 2021).

Ceci nous permettrait de faire ressortir certaines difficultés partagées, d'autres qui seraient propres au secteur concerné et ainsi de pouvoir tirer des conclusions plus générales sur la gestion de cette question au niveau belge.

3. Modèle d'analyse

Le modèle que nous utiliserons principalement est le « modèle PCP » proposé par Tanja A. Börzel (2021) dans son ouvrage « Why Noncompliance. The Politics of Law in the European Union ».

Ce modèle sera expliqué dans la partie théorique de ce mémoire mais en guise d'avant-goût, ce modèle explique la non-conformité sur base de trois critères : le pouvoir, la capacité et la politisation.

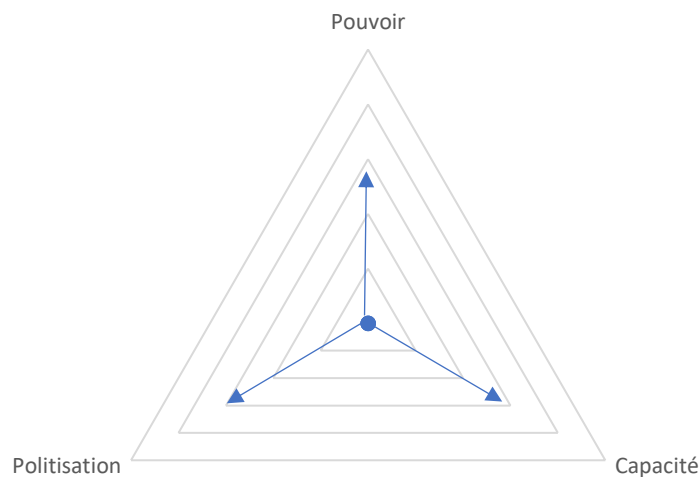


Figure 3: modélisation du modèle PCP

Ces trois critères seront au centre de notre analyse et nous permettront de déceler les raisons des difficultés de la Belgique dans le cadre de cette directive.

4. Collecte de données

Comme nous l'avons mentionné, l'objectif de ce mémoire est de faire ressortir les raisons derrière les difficultés de la Belgique par rapport à la directive NIS1. Nous devons pour ceci, analyser les secteurs qui ont dû faire face à cette problématique sur le terrain afin de faire apparaître ces raisons.

C'est pourquoi nous avons opté pour une méthode qualitative. Une approche quantitative ne serait pas adaptée dans le cas présent car nous devons avoir des données de fond qui nous pointent dans une direction et nous permettraient d'analyser le sujet méticuleusement selon la grille de Börzel (2021). Nous ne pouvons également pas nous permettre d'interroger chaque

entité concernée par la directive. Celles-ci sont assez vastes et impliquent tant des entités du secteur public que du secteur privé. La recherche aurait été trop laborieuse et inutilement longue dans ce cas (Van Campenhoudt et al., 2017).

La démarche qui nous permettrait de mieux répondre à nos interrogations est une démarche inductive. Le phénomène est déjà connu et cette démarche nous permet de mieux comprendre les raisons qui se cachent derrière celle-ci (Claude, 2021).

L'entretien nous permet d'avoir ces réponses recherchées en interrogeant les différents acteurs retenus dans le cadre de cette analyse en faisant ressortir l'expérience propre à cette entité.

Il est important néanmoins que nous précisions une chose. Le modèle de Börzel (2021) implique également deux concepts centraux de cette analyse : le « *shaping* » et le « *taking* » des Etats face à des normes internationales.

Si les entretiens nous permettent de répondre à la question du « *taking* », celles-ci ne pourront fournir que très peu d'indications quant au « *shaping* ». C'est pourquoi, afin de répondre à cette question, nous avons analysés divers documents (principalement des procès-verbaux du Parlement européen et du Conseil de l'Union européenne) pouvant nous indiquer potentiellement les réponses recherchées.

C. Hypothèse

Nous rappelons que notre analyse est principalement basée sur le modèle de Tanja A. Börzel (2021). Pour ceci, nous avons identifié deux points comme repris dans le point précédent : le « *shaping* » et le « *taking* ».

Ces deux points constituent la base de notre réflexion et de nos hypothèses. Au cours de nos recherches, un lien évident est apparu entre la non-conformité de la Belgique et les concepts identifiés. Ceci nous a amené à formuler deux hypothèses qui seront analysés dans le chapitre III de ce mémoire :

- 1) La Belgique n'était pas en mesure de faire face aux obligations de la directive NIS1 en interne car elle ne disposait pas de la capacité à implémenter ces nouvelles obligations.
- 2) La Belgique n'était pas assez impliquée au niveau des discussions législatives européennes ce qui ne lui a pas permis d'avoir une directive qui permettrait de réduire les coûts d'implémentation.

Chapitre 2 : Etat de l'art

A. Analyse de la directive NIS

1. Exigences de la directive

Nous avons déjà mentionné à plusieurs reprises la directive qui fera l'objet d'une analyse dans ce mémoire. Néanmoins, nous n'avons pas encore pu détailler ce qu'elle impliquait réellement. Afin de comprendre les enjeux auxquels les entités concernées par la directive font face, il est important de bien maîtriser son contenu.

Tout d'abord, avant toute chose, rappelons que la directive NIS1 propose une série de secteurs pouvant être considérés comme étant sous le champ d'application de la directive en son annexe II (*EUR-LEX - 32016L1148 - EN - EUR-LEX*, s. d.). La directive introduit deux notions centrales qui permettent de catégoriser les entités concernées par les obligations de celle-ci : les « opérateurs de services essentiels » et les « fournisseurs de services numériques ».

Néanmoins, la directive laisse le champ libre aux Etats membres afin de définir quels seront les secteurs retenus sur son propre territoire. La directive NIS a été transposée en droit belge à travers la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. La Belgique a fait le choix d'inclure cinq secteurs parmi ceux présents dans l'annexe II de la directive NIS à savoir :

- l'Energie ;
- le Transport ;
- les Finances ;
- la Santé ;
- l'eau potable ;
- les infrastructures numériques.

Les critères d'identification des OSE et FSN sont décrites au chapitre 1^{er} de cette même loi.

Selon les risques propres à chacun des secteurs, les entités devront veiller à avoir une sécurité plus poussée afin de toujours garantir une continuité de service aux citoyens. Les Etats membres, en plus de devoir transposer la directive dans la législation nationale devront également adopter une stratégie cybersécurité qui définit les priorités à venir (Mathias, 2018).

La définition des entités potentiellement concernés est cependant souvent lacunaire et oblige les Etats à définir eux-mêmes les critères d'application de la directive (Mathias, 2018).

La directive vise à renforcer la résilience numérique des Etats grâce à plusieurs objectifs (Quéméner (2016) :

- La création d'une autorité nationale de cybersécurité
- La désignation d'équipes d'interventions aux incidents informatiques (CSIRT)
- Le développement des stratégies cyber nationales

Néanmoins, bien que cette directive impose des obligations importantes aux Etats membres, elle en impose aussi indirectement aux acteurs de terrain concernés tels que les OSE et FSN.

La loi belge du 7 avril 2019 n'impose pas de mesures de sécurités techniques spécifiques aux entités concernées. Au contraire, elle se limite à énumérer plusieurs points généraux aux articles 20 et suivants :

- L'adoption de mesures de sécurité techniques et organisationnelles garantissant un niveau de sécurité physique et logique adapté aux risques existants, compte tenu de l'état des connaissances techniques afin de protéger l'entité contre les risques qui la menacent ;
- L'élaboration d'une politique de sécurité répondant aux critères du point précédent ;
- Prouver sa conformité grâce à des audits de certification (ISO ou autre norme internationale) ;
- Désigner un point de contact qu'elle communique à l'autorité nationale (CCB) ;
- Notifier les incidents de sécurité « *ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit* » (Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique).

Ces obligations restent vagues et ne donnent pas une indication claire sur les mesures à mettre en place. C'est pourquoi la loi comporte la mention de normes de certifications afin d'aider les entités à faire face à ces défis.

2. Processus d'adoption

Bien que la directive ait été transposée en Belgique en 2019, celle-ci a connu un parcours législatif important au niveau européen. Cette procédure est résumée telle que suit (*EUR-LEX* – 32016L1148 – EN – *EUR-LEX*, s. d.) :

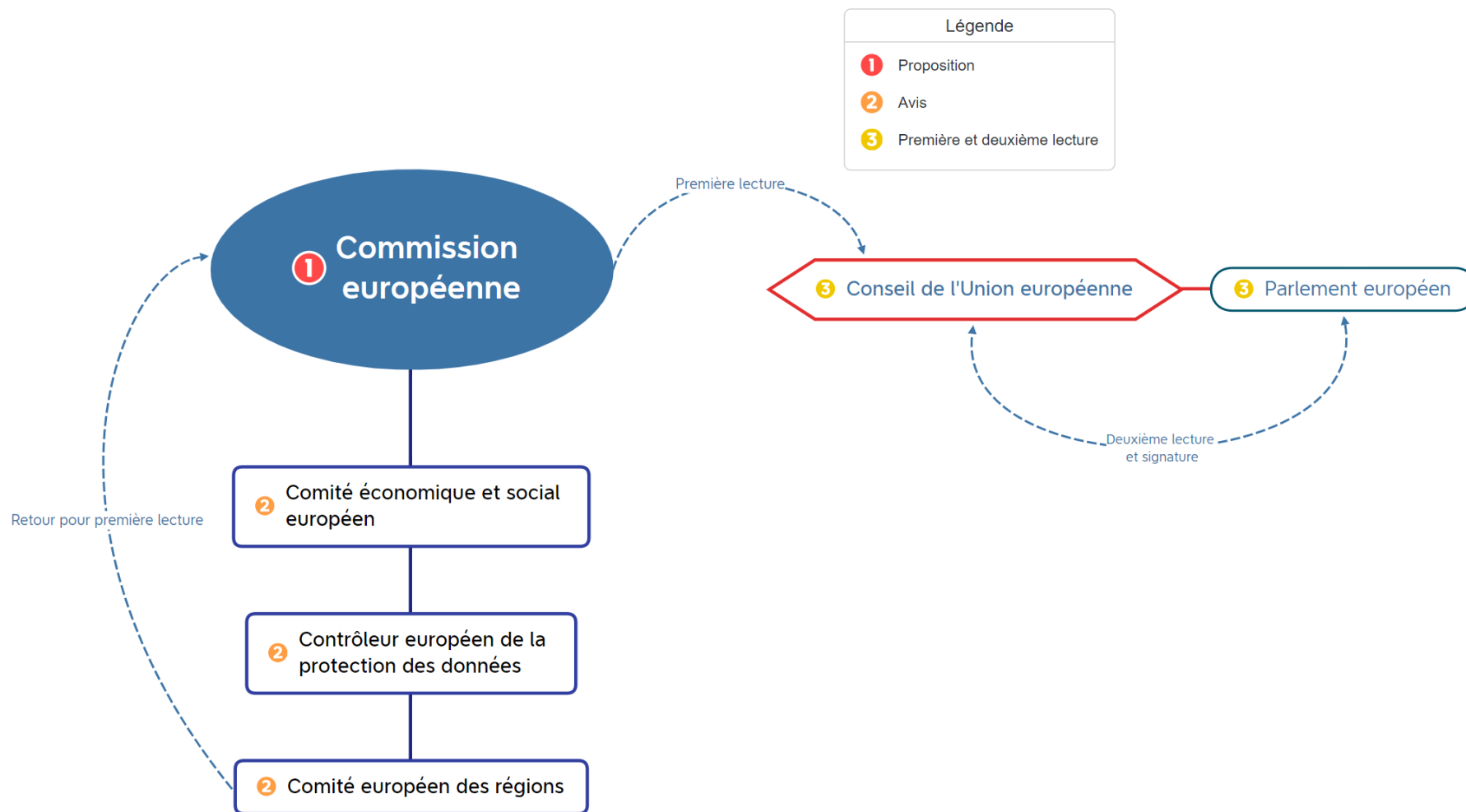


Figure 4: Résumé du processus législatif de la directive NIS 1

B. La « compliance » en politiques publiques

La conformité (souvent appelée « compliance ») a suscité un vaste intérêt au sein d'une littérature interdisciplinaire qui sera présentée et discutée dans ce chapitre. Un grand nombre d'études empiriques ont été menées sur ce sujet et il est nécessaire de développer un cadre théorique cohérent qui puisse prendre en compte les multiples facteurs interagissant et contribuant à la « compliance ». Ainsi, ce chapitre essaie d'exposer et d'examiner les principales approches théoriques qui ont été explorées au cours des dernières années, dans le but de fournir une compréhension plus approfondie.

Les lois et les directives communautaires sont intégrées et mises en pratique au sein des codes juridiques des États membres de l'Union européenne. L'objectif principal est de définir les notions d'« implémentation » et de « directive ». Les théories qui permettent de comprendre le processus de modification du droit des États membres sont examinées sous l'influence du droit communautaire. Duina (1997) analyse ces théories avec une attention particulière est accordée à l'hypothèse du coût, dont la validité est examinée. En outre, l'auteur analyse l'application des réglementations communautaires en matière d'égalité des salaires entre les sexes. (Duina, 1997).

L'intégration européenne conduit à une convergence dans la politique intérieure des États membres de l'Union européenne. Certaines études récentes affirment que l'intégration européenne conduit à une similitude croissante des politiques nationales des États membres. Cependant, l'introduction de diverses exemptions et dispositions de "flexibilité" dans les traités de Maastricht et d'Amsterdam, ainsi que les problèmes croissants de mise en œuvre, semblent contredire cette perspective. Dimitrova et Steunenberg (2000) exposent dans un article un modèle basé sur les choix publics, la théorie des jeux et la politique analytique pour expliquer les conditions dans lesquelles la convergence peut se produire et les limites de ce processus aux stades législatif et de mise en œuvre de la politique européenne. Au stade législatif, le modèle met en évidence la difficulté pour le Conseil, qui décide à l'unanimité, de parvenir à une politique uniforme, en particulier lorsque les politiques actuelles des États membres diffèrent considérablement. En ce qui concerne la mise en œuvre, les problèmes de mise en œuvre sont abordés en mettant l'accent sur les divergences de points de vue des acteurs politiques nationaux à l'égard de la législation européenne. En conclusion, il est souligné que la convergence ne se produira que lorsque l'Union sera en mesure d'établir une politique commune sans aucune

dérogação, qui sera ensuite pleinement mise en œuvre par les acteurs politiques nationaux. (Dimitrova & Steunenberg, 2000).

Cependant, quelles sont les raisons qui poussent les Etats à se conformer aux normes des régimes et institutions internationales ? Deux réponses concurrentes à cette question de la conformité ont été proposées par Checkel (2001) : l'approche rationaliste et l'approche constructiviste. Les rationalistes mettent l'accent sur la coercition, les calculs coûts/avantages et les incitations matérielles, tandis que les constructivistes insistent sur l'apprentissage social, la socialisation et les normes sociales. Ces deux approches expliquent des aspects importants de la conformité. Afin de trouver un lien entre elles, l'auteur examine le rôle de la persuasion argumentative et de l'apprentissage social. Cela permet de mettre en évidence la théorie du choix social et de l'interaction implicite présente dans de nombreuses études constructivistes sur la conformité, et d'élargir les arguments rationalistes concernant les processus instrumentaux et non instrumentaux par lesquels les acteurs se conforment. L'auteur soutient également que la politique intérieure, en particulier les contextes institutionnels et historiques, limite le rôle causal de la persuasion et de l'apprentissage social, ce qui aide les rationalistes et les constructivistes à préciser la portée de leurs affirmations sur la conformité. Pour évaluer la plausibilité de ces arguments, Checkel (2001) examine pourquoi les États se conforment aux nouvelles normes de citoyenneté/adhésion promues par les organisations régionales européennes.

Le débat contemporain concernant le respect des règles se focalise sur deux perspectives opposées quant à la meilleure approche pour amener les États à respecter les règles internationales : l'application et la gestion. Les théoriciens de l'application mettent l'accent sur une stratégie coercitive de surveillance et de sanctions, tandis que les théoriciens de la gestion adoptent une approche axée sur la résolution des problèmes, reposant sur le renforcement des capacités, l'interprétation des règles et la transparence. La conception selon laquelle l'application et la gestion sont des stratégies concurrentes pour atteindre le respect des règles est remise en question par Tallberg (2002). À partir de l'étude du cas de l'Union européenne (UE) et d'une comparaison avec d'autres régimes internationaux, Tallberg (2002) suggère que les mécanismes d'application et de gestion sont plus efficaces lorsqu'ils sont combinés. La combinaison d'instruments coopératifs et coercitifs dans une « échelle de gestion et d'application » permet à l'UE de lutter avec succès contre les violations, réduisant ainsi la non-conformité à un phénomène temporaire. L'analyse des régimes dans les domaines du commerce, de l'environnement et des droits de l'homme apporte un soutien supplémentaire à cette

proposition : les systèmes de conformité qui intègrent les deux formes de mécanismes sont particulièrement efficaces pour garantir le respect des règles, tandis que les systèmes qui se basent uniquement sur l'une des stratégies souffrent de limitations identifiables. (Tallberg, 2002).

Selon une perspective intergouvernementale, les problèmes de mise en œuvre surviennent lorsque les États membres ne parviennent pas à défendre leurs intérêts dans le processus décisionnel européen. En se concentrant sur 26 procédures d'infraction dans le domaine du droit du travail, une étude importante dans le thème de la compliance met en évidence l'existence occasionnelle d'une « opposition par la porte arrière ». Cependant, il est démontré que l'opposition à la fin du processus politique de l'UE peut également survenir sans opposition préalable au début. De plus, les résultats indiquent que la non-conformité est souvent due à des lacunes administratives, des problèmes d'interprétation et des problèmes de liaison, et n'est pas nécessairement liée à l'opposition. Cette étude repose sur des données approfondies et uniques provenant d'une analyse sur le terrain de la mise en œuvre de six directives européennes dans les 15 États membres. (Falkner, Hartlapp, Leiber & Treib, 2004)

Le néofonctionnalisme a été au cœur de l'explication de l'« élargissement des tâches » de la Communauté européenne. Alors que les études antérieures se sont principalement concentrées sur le transfert de compétences du niveau national au niveau européen, Börzel (2005) examine également les procédures de prise de décision au niveau européen (« portée »). La distinction entre la portée et le niveau révèle un puzzle intéressant. Il est largement reconnu que l'intégration de la sécurité extérieure et intérieure a progressé plus lentement. Depuis le traité de Maastricht, nous avons observé une expansion significative des responsabilités de l'UE dans ces deux domaines qui sont des bastions de la souveraineté nationale. Cependant, bien que le niveau d'intégration atteint soit assez similaire, la portée de l'intégration diffère considérablement. La justice et les affaires intérieures ont été intégrées dans le cadre supranational du premier pilier. En revanche, la politique étrangère et de sécurité commune ainsi que la politique européenne de défense restent fermement ancrées dans le domaine de l'intergouvernementalisme. Cette disparité entre le niveau et la portée de l'intégration européenne présente un défi théorique majeur pour le néo fonctionnalisme. (Börzel, 2005).

Une première étude empirique globale et approfondie sur les effets des politiques "volontaristes" et partiellement "douces" de l'UE dans les 15 États membres a été réalisée par Falkner, Hartlapp, Leiber et Treib (2005). En examinant 90 études de cas portant sur différentes directives européennes, il apporte des éclaircissements sur les questions contemporaines en

science politique, en théorie de l'intégration et en politique sociale. Les résultats de l'étude concluent à une prédominance de graves échecs de mise en œuvre et soulignent que jusqu'à présent, la Commission européenne n'a pas été en mesure d'assurer adéquatement sa fonction de contrôle. (Falkner, Hartlapp, Leiber & Treib, 2005). Dans cet ouvrage, la typologie des « 3 mondes de la compliance » a été élaborée.

Un article par Falkner, Hartlapp et Treib (2007) résume également les principaux résultats théoriques d'un projet qualitatif à grande échelle sur la transposition, la mise en œuvre et l'application de six directives de l'Union européenne sur le droit du travail dans 15 États membres. En se concentrant sur la phase de transposition, l'argumentation part d'une énigme théorique : lorsque l'on confronte les résultats empiriques des 91 cas couverts par l'article avec les différentes hypothèses dérivées de la littérature, il s'avère que toutes les conditions causales suggérées par les théories existantes, et même deux des hypothèses les plus importantes (sur l'inadaptation et les acteurs du veto), ont au mieux un pouvoir explicatif plutôt faible. En y regardant de plus près, ces études qualitatives montrent que même leur raisonnement de base ne tient pas dans certains groupes de pays. Comme solution, cet article propose une typologie de trois mondes de conformité, chacun d'entre eux étant caractérisé par un style de transposition idéal-typique : un « monde de respect de la loi », un « monde de politique intérieure » et un « monde de négligence de la transposition ». (Falkner, Hartlapp & Treib, 2007).

Cette typologie fournit la clé pour comprendre quand et comment les propositions théoriques individuelles sont pertinentes. (Falkner, Hartlapp & Treib, 2007) :

	Monde de l'observation de la loi	Monde des politiques domestiques	Monde de la négligence de la transposition
Déroulement de la transposition	Transposition à temps et fidèle (même si conflit avec une norme interne)	S'il n'existe pas de conflit interne avec des préoccupations nationales, la transposition est faite à temps	Lente et superficielle
Conditions de non-conformité	L'Etat n'est pas au courant de la politique (rare)	Echec politique (pas de compromis réalisé)	Echec bureaucratique
Facteurs facilitants la conformité	Culture de conformité présente	Adapté aux préférences étatiques	Accélérer le lien avec des réformes internes

Tableau 1 : Adapté de "Three worlds of compliance" (Falkner, Hartlapp & Treib, 2007)

La phase de négociation précédant l'adoption d'accords internationaux sur la phase ultérieure de mise en œuvre est également un facteur important à prendre en considération. Cette question est abordée par Thomson et al. en examinant les liens entre la prise de décision sur les directives de l'Union européenne et les infractions ainsi que les retards ultérieurs dans la transposition nationale. Il est proposé une explication de la non-conformité basée sur les préférences, qui met l'accent sur les incitations des États à s'écarter des directives et sur la marge de manœuvre qui leur est accordée. Cette hypothèse est comparée aux explications basées sur les caractéristiques spécifiques de chaque pays. Les infractions sont plus probables lorsque les États ne sont pas en accord avec le contenu des directives et lorsqu'ils disposent de peu de marge de manœuvre. Cependant, l'octroi d'un pouvoir discrétionnaire aux États membres tend à prolonger les délais de transposition. Néanmoins, aucune preuve d'effets spécifiques aux pays n'a été trouvée dans cette étude. (Thomson, Torenvlied & Arregui, 2007).

Une étude réalisée par Toshkov (2007) a néanmoins testée l'argument selon lequel le classement des pays dans trois univers de conformité permet d'expliquer les performances en matière de transposition au sein de l'Union européenne. L'étude examine les caractéristiques culturelles qui distinguent les mondes de la "culture de la conformité" et cherche à déterminer si les

attitudes à l'égard du respect des lois et des règles, ainsi que la confiance dans les institutions de l'UE, sont directement liées à l'appartenance à ces trois types de mondes. Les résultats montrent que ces attitudes ne sont pas directement liées à l'appartenance à ces univers de conformité. Ensuite, l'étude se concentre sur le potentiel explicatif de la typologie et observe que les niveaux de non-transposition sont cohérents avec l'argument avancé, bien que les différences entre les groupes ne soient que marginalement significatives. Cependant, l'analyse empirique des données annuelles spécifiques à la politique concernant les taux de non-transposition pour la période allant de 1998 à 2005 ne confirme pas les implications de la typologie en ce qui concerne la variabilité des performances de transposition et l'impact différencié de la politique intérieure dans les mondes de la conformité. (Toshkov, 2007).

En se basant sur les résultats d'une étude antérieure portant sur la conformité dans les 15 États membres « anciens » de l'Union européenne (cf. supra), qui a identifié trois « mondes de conformité », Falkner et Treib (2008) tentent de déterminer si les nouveaux États membres d'Europe centrale et orientale représentent ou non un monde de conformité distinct. Pour ce faire, les auteurs présentent les résultats empiriques d'un projet de recherche portant sur la mise en œuvre de trois directives européennes concernant le temps de travail et l'égalité de traitement dans quatre pays d'Europe centrale et orientale. Les preuves suggèrent que les nouveaux États membres présentent des styles de mise en œuvre similaires à ceux de certains pays des 15 États membres de l'UE. Les études de cas réalisées ne confirment pas l'hypothèse selon laquelle les nouveaux États membres pourraient adopter une logique distincte, par exemple en réduisant considérablement leurs efforts de mise en conformité après leur adhésion pour se "venger" de la pression exercée par la conditionnalité. Au contraire, les quatre nouveaux États membres semblent appartenir à un groupe que l'on pourrait qualifier de « monde des lettres mortes ». Il est toutefois important de souligner que ce « monde de la conformité » spécifique, caractérisé par des processus de transposition politisés et des problèmes systématiques d'application et de mise en œuvre, comprend également deux pays parmi les 15 États membres « anciens » de l'UE. (Falkner & Treib, 2008).

Dans le même ordre d'idées, une comparaison réalisée par Falkner (2010) tente de mettre en évidence les performances des institutions publiques et le respect du droit européen dans quatre pays d'Europe centrale : la République tchèque, la Hongrie, la Slovaquie et la Slovénie. Les institutions publiques examinées, telles que le système judiciaire, les inspections du travail et les autorités chargées de l'égalité de traitement, jouent un rôle crucial dans l'application des normes sociales de l'UE. Les évaluations des experts et des praticiens révèlent des lacunes

significatives dans les performances institutionnelles de ces pays. Le schéma de conformité procédurale observé dans ces pays présente des similitudes avec celui identifié dans des études antérieures menées dans certains pays d'Europe occidentale, tels que l'Irlande et l'Italie. Ainsi, les quatre pays examinés ici sont considérés comme faisant partie d'un « monde de lettres mortes » en ce qui concerne le respect du droit communautaire. Dans ce "monde", la transposition des directives de l'UE est souvent politisée, bien que jusqu'à présent elle ait été effectuée dans les délais et de manière appropriée. Les cas de non-conformité deviennent fréquents aux étapes ultérieures de contrôle et d'application. En résumé, cet article met en évidence les lacunes des institutions publiques dans la République tchèque, la Hongrie, la Slovaquie et la Slovénie en ce qui concerne le respect du droit européen. Ces pays sont caractérisés par une transposition politisée des directives de l'UE et des problèmes de non-conformité à des stades ultérieurs du processus de contrôle et d'application. (Falkner, 2010).

La recherche sur la mise en œuvre des politiques de l'UE a connu des avancées théoriques, conceptuelles et empiriques substantielles ces dernières années. Cependant, les résultats obtenus restent ambivalents et les idées théoriques sont encore disparates. Il est donc nécessaire de se pencher sur certaines questions qui préoccupent ce domaine de recherche et de reconnaître les limites des différentes approches théoriques et des données couramment utilisées. Un aspect important concerne les défis liés à l'opérationnalisation et au choix d'indicateurs appropriés pour mesurer la conformité (« compliance ») en tant que variable dépendante. Il est crucial de déterminer quels indicateurs sont les plus pertinents pour évaluer le respect des lois et des politiques de l'UE. De plus, il est essentiel d'explorer les avantages et les pièges des différents types de données utilisées dans ce domaine, tels que les statistiques officielles sur les notifications et les infractions publiées par la Commission européenne, ainsi que les données issues d'enquêtes de masse. La recherche sur la mise en œuvre de l'UE a indéniablement progressé sur les plans théorique, conceptuel et empirique ces dernières années. Cependant, les résultats obtenus demeurent ambivalents et les connaissances théoriques sont encore fragmentées. Par conséquent, il est nécessaire d'identifier les domaines problématiques de cette branche de recherche et d'accroître la sensibilité aux différentes approches méthodologiques et aux types de données utilisés. Cela implique notamment de mieux définir les concepts clés et de choisir des indicateurs appropriés pour expliquer la variable dépendante (le respect des lois). De plus, il convient de se pencher sur les avantages et les inconvénients des différentes sources de données utilisées dans la plupart des études, notamment les statistiques officielles sur les

notifications et les procédures d'infraction publiées par la Commission européenne, ainsi que les données issues d'enquêtes. (Falkner & Hartlapp, 2009).

Il est tout de même important de rappeler que l'Union européenne (UE) n'est pas un système de gouvernance aussi unique que ce que sa diversité d'étiquettes peut suggérer. Tout comme ses États membres, l'UE présente une combinaison de différentes formes de gouvernance qui s'étendent de l'échelle du marché à celle de la hiérarchie. Cependant, contrairement au niveau national, on observe très peu de formes de gouvernance en réseau au sein de l'UE, impliquant systématiquement des acteurs privés. La gouvernance de l'UE est principalement régie par des accords négociés entre des acteurs intergouvernementaux et transgouvernementaux. Alors que les entreprises, les groupes d'intérêt ou les organisations de la société civile ont rarement leur mot à dire dans l'élaboration des politiques européennes, les mécanismes de concurrence politique fondés sur le marché ont gagné en importance. Ainsi, l'UE se caractérise moins par une gouvernance en réseau où les acteurs privés sont fortement impliqués, que par des négociations intergouvernementales et transgouvernementales d'une part, et par une concurrence politique entre les États membres et les régions d'autre part. Ces deux aspects opèrent dans l'ombre de la hiérarchie établie par les institutions supranationales de l'UE. En résumé, l'article remet en question l'idée que l'UE est un système de gouvernance en réseau et met en avant le rôle prépondérant des négociations entre acteurs intergouvernementaux et transgouvernementaux, ainsi que la concurrence politique entre les États membres et les régions, comme principales caractéristiques de la gouvernance de l'UE. (Börzel, 2010).

Les variations entre les pays en ce qui concerne la non-conformité au droit européen sont également un facteur dont il faut tenir compte. Bien que la non-conformité n'ait pas connu une augmentation significative au fil du temps, certains États membres de l'Union européenne enfreignent plus fréquemment le droit européen que d'autres (voir « mondes de la conformité »). Börzel et al. (2010) se basent sur trois approches principales largement utilisées dans la littérature sur la conformité : l'application, la gestion et la légitimité. Ils développent des hypothèses pour chaque approche avant de les combiner de manière cohérente sur le plan théorique. Ces hypothèses sont ensuite testées empiriquement à l'aide d'un ensemble complet de données portant sur plus de 6300 violations du droit européen. Les résultats de l'étude mettent en évidence l'importance de combiner les approches de l'application et de la gestion. Les États membres puissants sont les plus susceptibles de violer le droit européen, tandis que les petits pays dotés d'une bureaucratie efficace sont les meilleurs observateurs. Cependant, la capacité administrative joue également un rôle pour les États membres puissants. Par exemple, le

Royaume-Uni respecte beaucoup plus la législation européenne que l'Italie, malgré un pouvoir politique similaire, en raison de l'efficacité de sa bureaucratie. En résumé, cet article soutient que la non-conformité au droit européen varie d'un pays à l'autre. Les facteurs tels que la puissance politique, la capacité administrative et l'efficacité de la gestion jouent un rôle crucial dans la détermination du niveau de respect du droit européen par les États membres de l'Union européenne. (Börzel, Hofmann, Panke & Sprungk, 2010).

Le lien entre l'élaboration des politiques de l'Union européenne (UE) et leur mise en œuvre, en mettant l'accent sur le rôle des parlements nationaux est un facteur important de la « compliance ». Alors que de nombreuses études se sont concentrées sur le non-respect de la législation de l'UE, peu ont cherché à comprendre comment la phase d'élaboration des politiques influence la mise en œuvre et s'il existe un lien de causalité entre les deux étapes. Sprungk (2011) propose dans un article un cadre théorique qui identifie trois mécanismes de causalité reliant l'élaboration des politiques à leur mise en œuvre : l'affirmation de soi, l'équité et l'information. Ces mécanismes expliquent comment les décisions prises lors de l'élaboration des politiques peuvent influencer la manière dont elles sont mises en œuvre ultérieurement. Pour tester empiriquement ces mécanismes, l'article se penche sur l'implication des parlements nationaux dans la négociation et la transposition de la directive-cadre sur l'eau. En examinant les cas de l'Assemblée nationale et du Bundestag, il évalue dans quelle mesure ces mécanismes de causalité sont présents et influents. Les résultats des études de cas montrent que le lien de causalité entre l'élaboration des politiques et la prise de décision est plus probable lorsque les acteurs restent les mêmes, lorsque peu de temps s'écoule entre les deux étapes et lorsque l'implication des acteurs de la mise en œuvre dans l'élaboration des politiques se concentre sur la fourniture d'informations. En résumé, cet article théorise et teste empiriquement le lien entre l'élaboration des politiques de l'UE et leur mise en œuvre, en se concentrant sur les parlements nationaux. Il identifie trois mécanismes de causalité et démontre leur influence en se basant sur des études de cas spécifiques. Ces résultats contribuent à une meilleure compréhension des facteurs qui influencent la mise en œuvre des politiques de l'UE. (Sprungk, 2011).

Une étude réalisée par Angelova et al. (2012) propose une synthèse des recherches existantes sur la conformité aux directives européennes en se basant sur des approches quantitatives et qualitatives. L'objectif est d'identifier les arguments théoriques testés dans ces études, d'évaluer la robustesse de leurs résultats et de déterminer leur représentativité. Les chercheurs ont identifié 12 arguments théoriques différents dans un total de 37 études sur la conformité publiées. Ces arguments portent sur des aspects tels que la "bonne adéquation" (« goodness of

fit »), la prise de décision institutionnelle, les préférences politiques des acteurs et l'efficacité administrative. En examinant les résultats de ces études, les auteurs ont évalué leur robustesse et leur fiabilité. La synthèse révèle que les arguments de "bonne adéquation" et de "prise de décision institutionnelle" bénéficient de résultats solides et robustes. Cependant, les résultats concernant les "préférences politiques des acteurs" et "l'efficacité administrative" restent ambigus, ce qui signifie qu'ils ne fournissent pas de conclusions claires et unanimes. Une analyse plus approfondie de la conception des études a également révélé des effets de sélection des politiques et des pays. Par exemple, la plupart des études se concentrent sur les politiques environnementales et sociales, tandis que les pays scandinaves en conformité et les pays du Sud en non-conformité sont rarement inclus dans les échantillons de recherche. Sur la base de ces résultats, les chercheurs recommandent d'interpréter les résultats existants sur la conformité avec prudence. Ils soulignent également l'importance d'une sélection plus attentive des pays et des domaines politiques dans les futures recherches sur la conformité aux directives européennes. En résumé, cette étude fournit une synthèse des recherches existantes sur la conformité aux directives européennes, en évaluant la robustesse des arguments théoriques et la représentativité des résultats. Elle souligne les résultats solides pour certains arguments, tout en soulignant les lacunes et les effets de sélection observés dans la recherche existante. (Angelova, Dannwolf & König, 2012).

Une non-conformité ne peut cependant pas être attribuée à des lacunes législatives. Dans son étude, Batory (2012) vérifie cette hypothèse en analysant la législation anti-corruption dans les États d'Europe centrale et orientale. L'auteur se penche sur la question de la lutte contre la corruption dans les États d'Europe centrale et orientale membres de l'Union européenne. Malgré l'introduction de nombreuses mesures de lutte contre la corruption au cours des dernières décennies, ce phénomène persiste dans ces pays. Plutôt que de se concentrer sur les failles de la législation existante, l'article identifie les raisons pour lesquelles les individus censés se conformer à la loi ne le font pas. En s'appuyant sur les idées théoriques des études de mise en œuvre, l'article met en évidence le rôle des incitations et des jugements normatifs dans la non-conformité à la législation anti-corruption. Il observe que les incitations et les normes sociales favorisent souvent le comportement non conforme aux lois anti-corruption. Par exemple, certains acteurs peuvent être incités à s'engager dans des pratiques corrompues en raison des avantages qu'ils en retirent, ou parce que ces pratiques sont socialement acceptées. Les implications politiques de ces constatations sont que les initiatives de lutte contre la corruption devraient accorder une plus grande attention à la sensibilisation des groupes cibles. Il est

nécessaire de comprendre les normes sociales existantes et d'adapter les mesures de lutte contre la corruption en conséquence. En outre, les incitations positives devraient être utilisées pour encourager la conformité plutôt que de se concentrer uniquement sur l'augmentation des sanctions. Les incitations et les jugements normatifs jouent un rôle crucial dans le comportement des acteurs concernés. (Batory, 2012).

Les variations de réactions des États membres de l'Union européenne (UE) lorsqu'ils sont confrontés à des cas de violation du droit européen et font l'objet de poursuites sont aussi un point important de la compréhension de la « compliance ». Börzel et al. (2012) mettent en évidence les différences de comportement entre les pays, notamment le Portugal, l'Italie et la Belgique, dans leur manière de traiter les cas de non-conformité. Selon cette étude, le Portugal a tendance à résoudre rapidement les cas de non-conformité dès les premières étapes de la procédure officielle d'infraction de l'UE. En revanche, l'Italie et la Belgique adoptent une approche plus tardive, voire ne se conforment pas du tout aux arrêts de la Cour européenne de justice, même après avoir été condamnées à deux reprises pour violation du droit européen. L'article explore les principales théories de la conformité pour expliquer ces modèles divergents de non-conformité persistante dans les États membres de l'UE. Les auteurs formulent et testent un ensemble d'hypothèses qui cherchent à expliquer la dynamique de la non-conformité à travers les différentes étapes des procédures d'infraction de l'UE et dans le temps. Les résultats de l'étude suggèrent que les différences de capacité et de pouvoir expliquent la variation des schémas longitudinaux de non-conformité. Cela signifie que les pays qui ont une capacité institutionnelle et administrative plus forte ainsi qu'un pouvoir politique plus élevé sont susceptibles de présenter des comportements de non-conformité persistante. En résumé, cela met en évidence les variations de réactions des États membres de l'UE face aux cas de violation du droit européen. Les différences de capacité et de pouvoir jouent un rôle clé dans la compréhension de ces variations, et ces facteurs peuvent expliquer les schémas de non-conformité persistante observés dans certains pays. (Börzel, Hofmann & Panke, 2012).

La conformité à la mise en œuvre correcte et opportune des politiques dans un système à plusieurs niveaux est modélisée comme un jeu stratégique entre un organisme central de contrôle et plusieurs exécutants. La conformité est déterminée par la décision d'application anticipée de l'agence de contrôle, et cette agence est sensible à la probabilité de succès de l'application et aux coûts de sanction potentiels encourus par les exécutants en cas de non-respect des règles. En se concentrant sur le système de contrôle centralisé de l'Union européenne (UE), l'étude de König et Mäder (2013) vise à évaluer l'efficacité de ce système. Les résultats

rèvelent que l'agence de contrôle de l'UE s'abstient d'imposer la conformité lorsque la probabilité de réussite de l'application est faible et que les coûts de sanction sont élevés. Cela entraîne un déficit de conformité, même si les activités d'application sélective de l'agence de contrôle sont généralement couronnées de succès devant les tribunaux. En résumé, cette étude souligne que, malgré l'efficacité globale du système de contrôle centralisé de l'UE, l'agence de contrôle fait preuve de sélectivité dans son application des règles, en s'abstenant de poursuivre les cas où les chances de succès sont faibles et les coûts de sanction élevés. Cela peut conduire à un déficit de conformité dans certains cas. (König & Mäder, 2013).

Une idée répandue demeure tout de même en théories de « compliance » selon laquelle le respect de la législation de l'Union européenne par les États membres est principalement déterminé par le calendrier des mesures de mise en œuvre déclarées. Zhelyazkova (2015) souligne que le simple fait d'adopter précocement une mesure de mise en œuvre ne garantit pas automatiquement la conformité à la législation de l'UE. Zhelyazkova (2015) examine spécifiquement le processus de signalement par les États membres de la législation nationale adoptée pour signaler la mise en œuvre d'une directive de l'Union européenne. Les chercheurs se demandent si le signalement de mesures de mise en œuvre préexistantes, qui peuvent ne pas répondre pleinement aux objectifs de la directive, est associé à une non-conformité détectée par la Commission européenne. Les résultats révèlent que, sauf si les États membres font face à des coûts de réputation importants, ils ont tendance à signaler des mesures de mise en œuvre existantes qui ne sont pas nécessairement adaptées à la directive concernée, sans effectuer les ajustements nécessaires en temps voulu. Cette pratique indique des problèmes potentiels de conformité, ce qui conduit souvent la Commission européenne à ouvrir des procédures d'infraction pour examiner la situation plus en détail. En résumé, l'étude de Zhelyazkova (2015) met en évidence les limites de la simple adoption précoce des mesures de mise en œuvre déclarées en tant qu'indicateur de conformité à la législation de l'Union européenne. Elle souligne l'importance pour les États membres d'adopter des mesures de mise en œuvre appropriées et de procéder aux ajustements nécessaires pour atteindre les objectifs des directives de l'UE. L'absence de ces ajustements peut conduire à des problèmes de conformité et à l'ouverture de procédures d'infraction par la Commission européenne. (Zhelyazkova, 2015).

Au fil du temps, les trois approches classiques dominantes de l'intégration européenne (le libéral intergouvernementalisme, le néofonctionnalisme et le postfonctionnalisme) sont remises en question par Börzel et Risse (2017) qui affirment qu'elles ne parviennent pas à expliquer complètement les résultats très différents obtenus lors des deux crises les plus récentes de

l'Union européenne (UE). Selon les auteurs, le libéral intergouvernementalisme et le néofonctionnalisme peuvent expliquer pourquoi la crise de l'euro a conduit à une plus grande intégration, mais ils échouent à expliquer pourquoi l'UE est restée bloquée dans une impasse lors de la crise de Schengen liée aux questions de sécurité. En revanche, le postfonctionnalisme, qui met l'accent sur la dépolitisation par le biais d'une délégation supranationale, conduit à une plus grande politisation pendant la crise de l'euro. Pour résoudre cette énigme, l'auteur soutient qu'il est nécessaire de prendre en compte le rôle de la politique identitaire dans les deux crises. Les controverses politiques lors de la crise de l'euro se sont concentrées sur des questions d'identité européenne, de solidarité entre les membres et de définition de l'Europe en tant que communauté. En revanche, la crise de Schengen a été politisée par le discours populiste et eurosceptique, qui a mis l'accent sur les questions de frontières et a plaidé en faveur d'une "Europe forteresse" excluante. Les auteurs affirment que la prédominance de ces positions d'exclusion dans la politisation des affaires européennes a nui à la valorisation de l'intérêt commun européen dans la crise de Schengen. En conclusion, cette contribution souligne l'importance des dimensions identitaires et politiques dans la compréhension des résultats divergents des crises de l'UE. Elle met en évidence l'impact de la dépolitisation et de la politisation sélective ainsi que les différences dans les discours politiques sur l'identité européenne et la solidarité entre les membres de l'UE. (Börzel & Risse, 2017)

Enfin, aux fins de ce mémoire, une étude comparative entre le Danemark et de la Belgique en matière de transposition des directives environnementales de l'Union européenne (UE) semble tout à fait pertinente. Les statistiques de la Commission européenne révèlent des différences significatives dans la mise en œuvre de ces politiques entre les deux pays. Bursens (2002) cherche à expliquer ces différences en se concentrant sur les facteurs institutionnels nationaux. L'auteur écarte les explications basées sur des facteurs de niveau européen et souligne plutôt l'importance des contextes institutionnels nationaux. Pour ce faire, une approche institutionnelle est présentée, en mettant l'accent sur les institutions "dures" et "douces" en tant que variables explicatives. L'article examine sept catégories de variables pour expliquer les différences de performance : les facteurs "durs" comprennent le contexte constitutionnel et administratif (répartition des compétences et mécanismes de coordination), la capacité institutionnelle, la pression d'adaptation administrative et juridique, la communication et la continuité. Les facteurs "doux" incluent la jalousie institutionnelle, l'eupéanisation et la pression d'adaptation politique. L'étude constate que les deux pays étudiés affichent des scores différents pour presque toutes les variables examinées, ce qui suggère des conditions de mise en œuvre moins

favorables pour la Belgique et des conditions beaucoup plus favorables pour le Danemark. En résumé, l'article met en évidence l'importance des différences institutionnelles nationales pour expliquer les performances divergentes dans la mise en œuvre des politiques européennes. Il souligne la nécessité de prendre en compte les caractéristiques institutionnelles spécifiques de chaque pays lors de l'analyse de leur capacité à transposer les directives de l'UE. (Bursens, 2002).

C. **« Why non-compliance »**

1. Introduction

"*Why Noncompliance*" (Börzel, 2021) est un ouvrage qui explore l'histoire de la non-conformité au sein de l'Union européenne (UE) en se focalisant sur les États membres qui respectent ou ne respectent pas de manière constante le droit communautaire. L'auteure, Tanja A. Börzel, examine les raisons de cette situation et son impact sur la gouvernance tant au sein de l'UE que dans un contexte plus large.

L'ouvrage étudie en détail les différents groupes d'États non conformes tout au long de l'existence de l'UE, remontant à son histoire longue et variée. Börzel (2021) remet en question certaines prénotions dans la recherche sur la conformité de l'UE, notamment en réfutant l'idée que la non-conformité est principalement causée par les nouveaux États membres d'Europe centrale et orientale ou par les États membres eurosceptiques.

L'auteure se penche sur des questions telles que : pourquoi les États qui critiquent ouvertement l'UE ont-ils de meilleurs résultats en matière de conformité que ceux qui la soutiennent ? Pourquoi la non-conformité a-t-elle diminuée depuis les années 1990 malgré l'élargissement de l'UE et l'adoption de nouvelles lois ?

Börzel (2021) met en avant la politisation comme facteur explicatif souvent négligé dans la littérature et les études sur l'UE. Elle soutient que la controverse politique, combinée au pouvoir de vote et à la capacité administrative des États membres, explique la diminution de la non-conformité au droit communautaire depuis l'achèvement du marché unique. Elle souligne également que la non-conformité se concentre généralement dans les domaines où l'UE cherche à protéger les droits des citoyens.

"*Why Noncompliance*" remet donc en question les explications traditionnelles de la non-conformité dans l'UE et met en évidence l'importance de la politisation ainsi que du pouvoir de

vote et de la capacité administrative des États membres dans la compréhension de ce phénomène.

Comme précisé en introduction, l'objectif du mémoire est d'analyser les raisons qui ont pu pousser la Belgique à avoir un retard dans la transposition et l'application de la Directive NIS1. C'est pourquoi, le modèle « PCP » proposé par Börzel (2021) est tout à fait pertinent afin d'analyser cette situation.

2. Le modèle « PCP » (Pouvoir, Capacité et Politisation)

Le modèle PCP conceptualise la conformité comme un jeu à deux étapes sur deux scènes différentes. Afin d'expliquer la conformité, l'analyse de l'implémentation et de l'exécution au niveau domestique d'une politique publique n'est pas suffisante mais doit également tenir en compte la phase de négociation à un niveau supranational (européen). La règle générale de ce modèle est que chaque Etat fonde ses actions sur sa volonté propre ou sa capacité à agir. Le modèle tente donc d'expliquer pourquoi certains Etats sont moins « *compliant* » plutôt que d'expliquer pour certains le sont.

Le modèle PCP est basée sur la rationalité des acteurs. Ces acteurs agissent donc de façon à maximiser leurs profits et minimiser leurs coûts. Les Etats ont des besoins basiques tels que la sécurité, la prospérité, le respect des droits de l'homme, etc. mais également des préférences en matière de politiques publiques (protection de l'environnement, ouverture du marché, etc.). La « *compliance* » ou la « *non-compliance* » est donc une stratégie de ces Etats à assurer le résultat domestique souhaité d'une politique publique en fonction de leur capacité et leur pouvoir. Les acteurs créent les institutions qui permettent d'orienter les résultats de leurs préférences et étant que le modèle PCP est basé sur les choix stratégiques, il explique comment les institutions créent les coûts et bénéfices qui influencent les choix de « *non-compliance* » (Börzel, 2021).

i. Pouvoir

Le pouvoir est la capacité d'un Etat à façonner ses actions afin de favoriser le résultat souhaité. Les Etats plus « puissants » peuvent façonner par exemple une politique publique afin de le faire correspondre à une situation préexistante ce qui réduit les coûts de conformité. Dans cette même optique, les Etats plus « puissants » sont normalement plus « *compliance* » car ils ont la capacité de réduire les coûts en façonnant les politiques européennes.

Ce pouvoir peut également leur permettre de résister aux coûts de « *compliance* » ainsi que dissuader les autorités de contrôle (car celles-ci seraient moins enclines à infliger des sanctions à ces Etats). (Börzel, 2021).

ii. Capacité

Les Etats ont besoin de ressources suffisantes afin d'implémenter les normes européennes et internationales (expertise légale, technique, etc.). Les ressources financières d'un pays jouent également un rôle important. Cependant, ces ressources ne sont pas garantes d'implémentation car elles requièrent une coordination entre les acteurs d'un Etat. De ce fait, plus une bureaucratie est inefficace, plus la possibilité de « non-compliance » devient évidente. Finalement, un Etat doit avoir l'autonomie nécessaire de prendre les décisions indépendamment des intérêts des acteurs. Ceci implique que des Etats avec beaucoup d'acteurs ayant la capacité de veto sont généralement moins « compliant ».

La capacité d'un Etat peut donc être évaluée sur base de 3 facteurs :

- Les ressources
- L'efficacité bureaucratique
- L'autonomie domestique

Il faut tout de même prendre en considération que certaines normes requièrent plus de capacité que d'autres. (Börzel, 2021).

iii. Politisation

« Les normes internationales rencontrent fréquemment un manque de mécanismes d'application au niveau international, ce qui entraîne des coûts élevés en cas de non-respect. Par conséquent, les chercheurs se sont de plus en plus intéressés à la mobilisation sociale au niveau national comme moyen alternatif d'accroître les coûts associés à la non-conformité. Cette approche met l'accent sur la création de pressions sociales et sur les conséquences négatives résultant de « non-compliance » des normes. » (Börzel, 2021).

L'explication de la « non-compliance » (ou de la compliance) des Etats peut être également attribuée à des mouvements de résistances selon les politiques. Ces revendications sont souvent portées par des ONG, groupes d'intérêts, lobbys, etc. Ce phénomène peut aussi expliquer comment certains Etats sont forcés de ne pas respecter les normes internationales.

iv. « *Shaping* » et « *Taking* »

	« <i>Shaping</i> »			« <i>Taking</i> »		
Pouvoir	Réduction des coûts de « compliance » à travers des négociations	Augmentation des coûts de compliance si plus de supranationalisation		Résistance possible grâce au pouvoir de résister aux coûts de non-compliance	Moins de résistance envers les coûts de « compliance » grâce à une implémentation plus efficace	Plus de résistance à des politiques réglementaires si coûts de « compliance » élevés
Capacité	Réduction des coûts à travers des négociations efficaces	Réduction des coûts de « compliance » grâce des législations plus adaptées aux différents contextes	Obtention d'une politique réglementaire qui bascule les coûts vers l'étape du « <i>taking</i> »	Capacité de faire face aux coûts grâce à une efficacité bureaucratique importante et l'existence de peu de « <i>veto players</i> »	Capacité de faire face aux coûts grâce à une gestion plus efficace	Plus de capacité requise pour s'adapter à des coûts engendrés par des politiques réglementaires
Politisation	Réduction des coûts de « compliance » à travers des politiques qui lient les mains des acteurs européens	Réduction des coûts de « compliance » grâce à une législation déléguée par le niveau européen		Résistance due à des mobilisations internes causées par des implications parlementaires	Si notoriété plus importante, plus grande capacité de résister aux coûts de « compliance »	Plus de résistance possible si notoriété plus élevée
	Etats	Temps	Secteur	Etats	Temps	Secteur

Tableau 2 : Adapté de "PCP in a two-level compliance game across two stages" (Börzel, 2021).

Ce tableau établi par Börzel (2021) permet d'expliquer les deux niveaux présents dans le façonnage (« *shaping* ») et la prise (« *taking* ») des politiques européennes à savoir le niveau européen et le niveau domestique, qui varient à travers le temps et le secteur. Celui-ci constitue la base de la réflexion présente dans ce mémoire.

Certains Etats orientent par exemple les normes sur la scène européenne de par leurs poids dans le budget européen. Offrir de l'expertise à l'Union pour façonner les politiques à venir est également un moyen de s'assurer qu'on oriente les normes dans le sens que l'on souhaite pour ces Etats. (Börzel, 2021).

Au niveau domestique, les acteurs disposant d'un pouvoir de veto sont également importants. Ceci est encore plus pertinent dans le cas de directives qui nécessitent l'approbation de parlements nationaux. Plus un Etat comprend d'acteurs ayant un pouvoir de veto, plus le façonnage des normes est un avantage pour ceux-ci afin de réduire les coûts de mise en conformité. Le modèle PCP se focalise sur la politisation d'un phénomène plutôt que le nombre d'acteurs ayant la capacité de veto et introduit le concept des institutions européennes qui peuvent mitiger la capacité de façonnage d'un Etat membre. (Börzel, 2021).

En ce qui concerne le « *taking* », les Etats doivent implémenter les normes adoptées au niveau européen. A ce stade, deux choix s'offrent à eux : accepter les coûts de la mise en conformité ou résister le changement. Le pouvoir d'un Etat dicte aussi sa capacité à résister aux coûts de conformités (en dissuadant les autorités de contrôle par exemple). Les Etats puissants sont aussi moins susceptibles de subir de lourdes sanctions de par leurs poids sur la scène européenne. (Börzel, 2021).

Les Etats membres peuvent également manquer de capacité à implémenter les décisions européennes sur l'échelle nationale (cf. supra). Le rôle des acteurs ayant le pouvoir de veto est renforcé dans cette phase car ils peuvent bloquer la mise en conformité. (Börzel, 2021).

Le modèle de Börzel (2021) émet donc plusieurs conclusions :

- Les États puissants ayant une faible capacité et un faible niveau de politisation affichent plus de non-conformité que les États membres moins puissants, dotés d'une forte capacité et une forte propension à la politisation.
- Plus les institutions limitent le pouvoir de façonnage des États, rendent la résistance au respect plus coûteuse pour eux, préservent ou renforcent leur capacité à faire face aux coûts de mise en conformité et réduisent les risques de politisation des coûts de mise en conformité, moins le risque de non-conformité est élevé.
- Les secteurs politiques qui imposent des coûts plus élevés, étant plus susceptibles d'être politisés, attirent plus de non-conformité que les secteurs politiques qui sont moins exigeants pour la capacité de l'État et sont politiquement moins sensibles.
- Plus les États sont intégrés dans le droit communautaire, plus ils sont conformes.

- Moins l'UE et le droit communautaire sont légitimes, plus le risque de non-conformité est élevé.

Ces hypothèses seront celles testées dans le cadre de la Directive NIS à travers les entretiens réalisés.

D. La transposition de politiques publiques

Un autre aspect important à développer pour ce mémoire est l'analyse des études réalisées en « transposition de politiques publiques ». Alors que la « compliance » s'intéresse au respect d'une norme, la transposition s'intéresse plutôt aux mécanismes d'implémentation de celle-ci au sein d'un Etat à proprement parler. Plusieurs études se sont intéressées aux théories de transposition de politiques publiques, et un bref exposé de celles pertinentes aux fins de ce mémoire paraît importante.

La capacité des acteurs à négocier avec succès afin de promouvoir leurs préférences institutionnelles a évolué avec le temps, en fonction du contexte institutionnel spécifique. Les acteurs utilisent leur pouvoir de négociation dans le cadre des règles institutionnelles existantes pour modifier l'équilibre entre législation et délégation, ainsi que les règles régissant la délégation, en leur faveur, entre les changements formels des traités. Les préférences d'un acteur collectif en matière de délégation dépendent de sa capacité à influencer la politique par le biais de la délégation ou de la législation. La prédominance des préférences d'un acteur spécifique, dans un contexte où différents acteurs ont des préférences divergentes, dépend de son pouvoir de négociation dans le cadre des règles institutionnelles existantes. Cela signifie sa capacité à entraver ou à mettre son veto à la politique afin de modifier la répartition entre législation et délégation, ainsi que les règles de délégation. Bergström et al. (2007) se concentrent principalement sur le choix de la procédure, c'est-à-dire sur les luttes visant à déterminer si la délégation ou la législation doit être utilisée. Une attention secondaire est accordée au changement de procédure. Les auteurs examinent l'évolution du débat sur la comitologie et la mise en œuvre au cours de cinq périodes clés, et étudie comment les acteurs de ces périodes ont cherché à modifier l'équilibre entre législation et délégation, ainsi que les règles de délégation, en fonction de leurs préférences. Cela met en évidence l'importance de la capacité de négociation des acteurs dans le contexte institutionnel pour promouvoir leurs préférences institutionnelles. Il montre comment les acteurs cherchent à modifier l'équilibre entre législation et délégation, ainsi que les règles de délégation, en utilisant leur pouvoir de négociation. L'article de Bergström et al. (2007) met en évidence l'évolution du débat sur la comitologie et

la mise en œuvre au fil du temps, en soulignant les stratégies des acteurs pour influencer les décisions institutionnelles en fonction de leurs préférences.

Une description systématique et une explication des variations dans la mise en œuvre des politiques de l'Union européenne entre les États membres et les directives est fournie par une étude de Haverland et Marleen (2007). Les analyses reposent sur un ensemble de données nouvelles et originales comprenant des informations comparables sur le retard de transposition de presque toutes les directives sociales de l'UE en Allemagne, en Grèce, aux Pays-Bas, en Espagne et au Royaume-Uni. Les résultats de l'analyse révèlent que les États membres n'ont transposé les directives à temps que dans 42,7 % des cas, et 17,5 % ont dépassé le délai de plus de deux ans. On observe des variations modestes entre les domaines de la politique sociale, des différences plus marquées entre les pays et de fortes variations entre les domaines au sein de certains pays. L'étude identifie deux facteurs importants associés au retard de transposition. Premièrement, le besoin de coordination interministérielle est lié à des retards. Cela souligne l'importance d'une coopération efficace entre les ministères concernés dans le processus de mise en œuvre. Deuxièmement, l'inefficacité administrative est également associée à des retards de transposition. Cela suggère que des problèmes bureaucratiques peuvent entraver le processus de mise en œuvre des directives. L'analyse ne montre aucun lien entre le retard de transposition et le fait qu'une directive soit nouvelle ou une simple modification, la complexité de la directive ou l'implication du Parlement dans le processus de transposition. Ces facteurs semblent ne pas avoir d'impact significatif sur la performance de transposition. Cela suggère que les États membres peuvent anticiper certains défis potentiels liés à la mise en œuvre et prendre des mesures pour les atténuer. L'article conclut en soulignant la nécessité de mener des recherches supplémentaires pour comprendre si et pourquoi les États membres agissent de manière proactive pour prévenir les retards de transposition. (Haverland & Marleen, 2007).

De la même manière, un autre article présente les résultats d'une étude quantitative portant sur la transposition de 1 117 directives dans cinq États membres de l'Union européenne et huit secteurs politiques sur une période allant de 1978 à 2002 (Haverland, Van Warden & Steunenberg, 2011). L'étude met en évidence des différences significatives de performance entre les secteurs politiques, ce qui rend difficile la généralisation à partir d'études portant sur un seul secteur. Les résultats suggèrent que ces différences peuvent être partiellement expliquées par des variations systématiques entre les secteurs en ce qui concerne les délais de transposition accordés, la proportion de directives émanant du Conseil par rapport à celles de la Commission européenne, ainsi que les mesures légales de mise en œuvre utilisées. Plus

précisément, l'étude révèle que certains secteurs politiques ont tendance à accorder des délais de transposition plus longs que d'autres. De plus, la proportion de directives émanant du Conseil par rapport à celles de la Commission peut varier entre les secteurs, ce qui influence également les délais de transposition. En outre, les mesures légales de mise en œuvre utilisées diffèrent d'un secteur à l'autre, ce qui peut avoir un impact sur la rapidité et l'efficacité de la transposition. Ces résultats soulignent l'importance de prendre en compte les spécificités sectorielles lors de l'analyse de la transposition des directives. Les différences intersectorielles observées mettent en évidence la nécessité de tenir compte du contexte politique, juridique et administratif spécifique à chaque secteur lors de l'évaluation des performances de transposition. Il convient de noter que ces conclusions sont basées sur une étude portant sur une période antérieure à 2002. (Haverland, Van Warden & Steunenberg, 2011).

Certains pays européens ont assimilé les normes et l'identité de l'intégration européenne. Huelshoff et al. (2005) soutiennent que pour tester cette affirmation en analysant l'Allemagne qu'ils jugent faire partie de ces pays, et qu'il est approprié de se pencher sur le respect du droit européen en tant qu'indicateur du degré d'engagement européen de l'Allemagne. Les comportements liés au respect du droit européen sont considérés comme étant fortement contraints et influencés par les normes procédurales et substantielles reconnues et acceptées. L'essai souligne la nature mutuellement constitutive des normes, de l'identité et des intérêts, et soutient que cette dynamique est reflétée dans le système juridique européen bien établi. L'évolution et la légitimité du droit européen sont considérées comme répondant aux critères de formation de l'identité et de construction des intérêts des États membres, tels que décrits dans la littérature. Pour évaluer cette proposition, l'auteur examine plus de 1 600 cas d'infractions au droit communautaire entre 1962 et 1999, où la Commission européenne poursuit un État membre pour non-respect du droit européen. Les résultats montrent que l'Allemagne se trouve en moyenne dans la même situation d'infraction que d'autres pays tels que le Royaume-Uni, la Belgique, la France, l'Irlande et le Portugal, et moins bien que le Danemark, les Pays-Bas et le Luxembourg. Sur la base de ces données, l'essai conclut que l'Allemagne ne peut pas être considérée comme plus "européenne" que la plupart des autres États membres de l'Union européenne. Cela remet en question l'affirmation selon laquelle l'Allemagne aurait pleinement assimilé les normes et l'identité de l'intégration européenne. Il convient de noter que ces conclusions se basent sur des données datant jusqu'à l'année 1999 et que la situation actuelle pourrait différer. Une mise à jour des données et une analyse plus récente pourraient fournir une perspective plus complète sur la position de l'Allemagne par rapport à d'autres États membres

de l'UE en ce qui concerne le respect du droit européen et l'assimilation des normes de l'intégration européenne. (Huelshoff, Sperling & Hess, 2005).

La transposition de la législation de l'Union européenne (UE) dans les douze "nouveaux" États membres pendant la phase de post-adhésion mérite également une attention particulière. L'analyse réalisée par Knill et Tosun (2009), est basée sur le nombre de lettres de mise en demeure reçues par ces nouveaux États membres entre 2004 et 2007. Les résultats de l'analyse révèlent des variations significatives dans le comportement de transposition entre ces pays. Les pays les plus performants en termes de transposition sont la Lituanie, la Hongrie et la Slovaquie, tandis que la Bulgarie, la République tchèque et surtout la Roumanie présentent des niveaux de transposition moins efficaces. Ces constatations indiquent que le processus d'incorporation des dispositions européennes dans le droit national comporte des problèmes, soulignant l'existence de défis plus importants en ce qui concerne l'aspect pratique de la mise en œuvre. L'analyse descriptive met en évidence que l'échec de la transposition est principalement lié à trois facteurs : le degré de commerce avec l'UE, la capacité bureaucratique et l'alignement des politiques de pré-adhésion. Ces éléments jouent un rôle clé dans la capacité des nouveaux États membres à transposer efficacement la législation européenne. En conclusion, il est suggéré qu'à moyen terme, l'augmentation des capacités bureaucratiques et le renforcement des liens économiques avec l'UE peuvent contribuer à réduire les échecs de transposition. Ces mesures permettraient d'améliorer la mise en œuvre de la législation européenne dans les nouveaux États membres et de renforcer leur conformité aux normes et obligations de l'UE. (Knill & Tosun, 2009).

Une autre étude se concentre sur l'échec et le retard de transposition des directives communautaires dans les ordres juridiques nationaux des États membres de l'Union européenne (UE) sur une période allant de 1986 à 2002 (König & Luetgert, 2009). L'objectif est de distinguer les facteurs nationaux des facteurs liés à l'UE qui contribuent à ces retards. L'étude constate que l'échec de la notification des mesures de transposition est plus probable lorsque des conflits surviennent entre les États membres pendant le processus législatif de l'UE. Cela suggère que les différences de priorités et d'intérêts nationaux peuvent influencer la volonté et la capacité des États membres à transposer les directives dans les délais impartis. Les résultats révèlent également une variation considérable dans les modèles nationaux de délais de transposition. Certains pays connaissent des retards plus importants que d'autres. Des facteurs tels qu'une complexité accrue des directives, un recours plus fréquent à la législation parlementaire, ainsi que des structures politiques nationales plus fédéralistes et pluralistes sont associés à des délais de transposition plus longs. En résumé, cette étude met en évidence

l'importance des facteurs nationaux et des conflits entre États membres dans l'échec et le retard de transposition des directives de l'UE. Elle souligne également l'influence de la complexité des directives et des caractéristiques institutionnelles nationales sur les délais de transposition. Comprendre ces facteurs peut contribuer à améliorer la mise en œuvre de la législation de l'UE au niveau national. (König & Luetgert, 2009).

Les difficultés liées à la transposition des directives européennes par les États membres de l'Union européenne (UE) sont examinées dans une autre étude de Steunenberg (2006). L'accent est mis sur la coordination de la transposition au sein de l'arène politique nationale. On considère la coordination comme un jeu dans lequel des acteurs de haut niveau prennent des décisions politiques lorsque les acteurs de niveau inférieur ne sont pas en mesure de le faire. Selon le modèle proposé, il est constaté que les acteurs de niveau inférieur peuvent parfois exercer un pouvoir discrétionnaire lors de l'élaboration de la politique de transposition d'une directive. De plus, lorsque la coordination est assurée par un seul acteur, la politique de transposition peut différer de ce qui est spécifié dans la directive. Cependant, la participation de plusieurs acteurs de haut niveau dans le processus décisionnel peut entraîner une impasse, conduisant à une transposition littérale de la directive. En outre, les blocages entre les acteurs décisionnels peuvent retarder le processus de transposition. Deux cas de décision sur des directives européennes aux Pays-Bas, concernant la directive sur le cacao et les produits chocolatés ainsi que la directive sur les poules pondeuses, sont présentés pour illustrer ces mécanismes. L'analyse réalisée dans cette étude démontre que le cadre théorique développé contribue à une meilleure compréhension de la transposition des directives européennes. En mettant en évidence l'importance de la coordination et des interactions entre les différents acteurs politiques, il permet d'expliquer les variations observées dans le processus de transposition. En résumé, cette étude met en évidence le rôle essentiel de la coordination politique dans la transposition des directives européennes au niveau national. Elle souligne également l'impact du pouvoir discrétionnaire des acteurs de niveau inférieur et des blocages entre les acteurs décisionnels sur le processus de transposition. (Steunenberg, 2006).

Contrairement aux études existantes sur la transposition, une approche spécifique axée sur la politique pour expliquer comment les acteurs nationaux transposent les directives est mise en avant par Steunenberg (2007). Selon cette approche, le résultat de la transposition dépend de l'arène institutionnelle où se déroule le processus décisionnel et des intérêts des acteurs nationaux impliqués. Ces arènes institutionnelles peuvent varier du parlement aux ministères et aux agences nationales. Les acteurs nationaux sont considérés comme ayant un pouvoir de veto

spécifique à la politique, et leurs préférences peuvent conduire à deux réponses différentes aux exigences d'une directive. Premièrement, les acteurs nationaux peuvent choisir de transposer littéralement une directive, réduisant ainsi les écarts au minimum. Deuxièmement, ils peuvent adopter une interprétation non littérale de la directive, entraînant des écarts plus importants dans les limites autorisées par la Commission européenne. Pour illustrer ces réponses, deux cas de transposition de directives européennes sont présentés : la directive sur les produits du tabac et la directive sur le commerce des animaux. L'analyse de ces cas démontre que l'approche politique spécifique proposée dans cet article contribue à une meilleure compréhension de la transposition. Elle permet de clarifier la manière dont les ambitions formulées à Bruxelles sont concrétisées en politiques par les administrations nationales. (Steunenberg, 2007).

Le rôle de la Commission européenne dans le contrôle de la transposition et de la mise en œuvre des directives européennes est crucial comme précisé antérieurement. L'approche adoptée considère que la Commission, en tant qu'acteur politique, est influencée par ses propres préférences politiques qui façonnent sa manière d'assumer son rôle de contrôle. Les réponses de la Commission peuvent varier, allant du rôle de "gardienne des traités", où aucun changement n'est permis, à celui de "témoin silencieux", où les États membres ont la possibilité d'établir leurs propres politiques nationales divergentes. Ces différentes réponses sont en accord avec les résultats empiriques qui démontrent que la Commission est plutôt sélective dans le déclenchement des procédures d'infraction. On peut considérer que la Commission joue le rôle de "Grand Frère" en surveillant les États membres, mais cela ne devient évident que lorsque les intérêts sont en conflit et que la Commission reçoit un soutien suffisant de la part de la Cour européenne de justice ou des autres États membres. (Steunenberg, 2010).

Les performances en matière de transposition des directives de l'Union européenne varient considérablement d'un pays à l'autre et d'un secteur politique à l'autre au sein de l'UE. Steunenberg (2009) examine les efforts de transposition de quatre directives communautaires dans les 27 États membres, ces directives étant susceptibles de poser des difficultés majeures en termes de conformité au niveau national. En utilisant la méthode de la régression des risques proportionnels de Cox, nous constatons que le pouvoir discrétionnaire et l'adéquation juridique sont des facteurs significatifs pour expliquer la transposition. De plus, nous découvrons que les nouveaux États membres d'Europe centrale et orientale ne sont pas moins performants que le reste de l'UE en ce qui concerne les délais de transposition. Il est surprenant de constater que l'efficacité du gouvernement est en relation négative avec la conformité, tandis que les périodes d'absence de gouvernement opérationnel n'ont pas d'effet sur les délais de transposition. Nos

résultats mettent en évidence l'importance des facteurs juridico-administratifs pour assurer le respect de la législation européenne. (Steunenberg, 2009).

Chapitre 3 : Les processus de « *taking* » et de « *shaping* » par la Belgique dans le cadre de la directive NIS

A. Présentation du contexte

A travers le chapitre précédent, nous avons pu remarquer que la conformité aux directives européennes par les Etats membres pouvait varier d'un sujet à l'autre. Le cas qui nous intéresse ici relève cependant de la directive NIS, à savoir de la sécurité informatique des réseaux. Celle-ci, par l'objet même de son texte, oblige les organisations recensées comme étant des « opérateurs de services essentiels » à mettre en place toute une série de mesures de sécurité afin de garantir la continuité des services proposés aux citoyens européens dans le cas d'un incident cyber (ce qui ne limite pas le champ d'application aux attaques à proprement parler).

Ces organisations jouent donc un rôle central dans la mise en conformité de la Belgique par rapport aux exigences de la directive.

Au niveau national, trois catégories d'acteurs se retrouvent donc mêlées à cette mise en conformité à savoir :

- L'autorité nationale compétente en la matière : le Centre pour la cybersécurité de Belgique (CCB)
- Les opérateurs et fournisseurs de services essentiels : toute organisation répondant aux critères de l'annexe 1 de la directive NIS (cf. chapitre 1).
- Les experts : personnes justifiant d'un savoir, ou d'une expérience dans un domaine précis (par exemple : académiciens) pouvant orienter l'action publique sur base d'une argumentation scientifique.

Ces trois types d'acteurs ont donc été interrogés sur base de la grille d'analyse proposée par Börzel (2021) sur le « *shaping* » et « *taking* » des politiques européennes. Premièrement, la première hypothèse sera vérifiée sur le plan du « *taking* ». Pour rappel, les seules stratégies s'offrant aux Etats pour l'implémentation de directives est l'acceptation des coûts liées à celle-ci ou la résistance à celle-ci. Ensuite, la deuxième hypothèse relative au « *shaping* » sera vérifiée en prenant en compte l'implication de la Belgique dans ce processus au niveau européen.

Les entretiens ont pu révéler un ensemble de données intéressantes par rapport à la question de la conformité de la Belgique à la directive NIS.

B. Le processus de « taking »

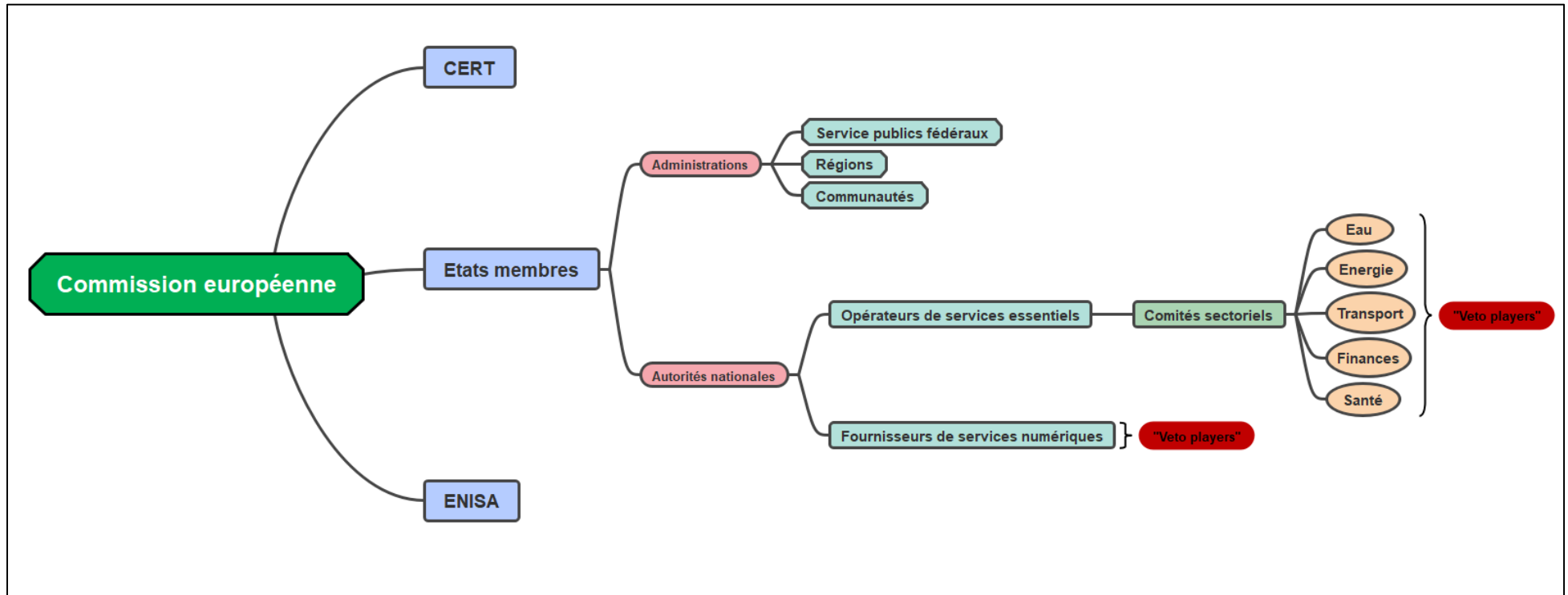


Figure 5 : Récapitulatif des acteurs concernés par la directive NIS

Il convient également d'analyser les acteurs impliqués dans le cas de la mise en conformité à la directive NIS. Comme nous l'avons vu au chapitre 2, la « Capacité » (modèle PCP) dépend de 3 facteurs (Börzel, 2021) :

- Les ressources
- L'efficacité bureaucratique
- L'autonomie domestique

A travers les entretiens, nous avons pu remarquer des manquements à ces 3 facteurs.

1. Les ressources

Afin de pouvoir déterminer les ressources disponibles pour la mise en conformité à la directive NIS, nous avons jugé intéressant d'interroger les acteurs de terrain concernés par son application direction. De ce fait, nous avons jugé intéressant d'interroger Digit'Eaux, la société responsable de l'informatique de la Société Wallonne des Eaux, étant la principale société de distribution et de production d'eau potable en Wallonie. Le responsable informatique, également en charge de l'implémentation des exigences de la directive NIS nous précise :

« il y avait déjà un retard d'une part au niveau de la transposition au niveau belge de la directive NIS et ça s'est encore accentué au niveau du secteur de l'eau par le fait qu'il n'y a pas de comité sectoriel où il n'existait pas de comité sectoriel au niveau du secteur de l'eau. Les banques, les secteurs de l'électricité, des transports, etc. ont un comité sectoriel qui peut animer les choses mais au niveau du secteur de l'eau, il n'en n'existait pas. Et donc le fédéral s'est tourné vers le SPW et la région flamande pour demander « comment fait-on ? ». Et le SPW a convoqué un peu toutes les entités, toutes les sociétés concernées, éventuellement pour dire « comment comptez-vous faire » et là il y a un souci, une lenteur assez conséquente de part justement ce manque de coordination globale. Entre temps c'est l'AFSCA qui a été nommée comme l'autorité sectorielle pour le secteur de l'eau. Mais à l'AFSCA, si vous me permettez l'expression, ils s'en fichent royalement de ce secteur de l'eau, ce n'est pas leur core business et donc quelque part ils sont un peu transparents et la conséquence est que maintenant arrive la directive NIS2 et on est à nouveau avec le même questionnement ».

Ce secteur s'est donc retrouvé sans soutien réel et a dû faire appel à de la consultance externe ce qui engendre des coûts assez importants, notamment au niveau des audits qui est une

obligation de la loi NIS (car renvoi à des normes de certifications existantes qui prévoient toutes des audits). Le responsable informatique nous précise également :

« Et là se pose la question : qui va financer les audits ? alors est ce que la consigne va venir du Fédéral pour avoir des sociétés qui vont nous auditer ou bien est-ce que chacun va créer son propre petit marché public pour chercher un auditeur ? Mais qui peut nous auditer ? alors là on tombe dans le fait même au niveau du secteur de l'eau est-ce qu'il existe bien des sociétés d'audit qui sont certifiées pour le secteur de l'eau (BELAC) ? J'ai eu une réunion avec le SPW où était également présent le CCB à qui j'ai posé la question et ils n'étaient pas en mesure de nous répondre ».

Ce point indique bien que le CCB et le Fédéral ne sont pas encore en mesure de faire face à toutes les inquiétudes pratiques du terrain posées par les exigences de la directive NIS. La nature même de la directive portant sur un sujet très technique, rend difficile la prise de décision par le CCB sur certains points. Le responsable informatique de Digit'Eaux nous précise :

« C'est quand même quelque chose de très informatique. Donc le fédéral s'est tourné vers le CCB qui a dit « mais moi je n'ai pas de pouvoir décisionnel » et donc on tourne un peu à tout niveau et je trouve un peu étonnant aussi, c'est que finalement ce sont les sociétés concernées qui doivent fixer les critères suivant lesquels on sera ou non nommé. ».

Un manque de ressources, au minimum, peut se déduire de ces déclarations.

La question avait été posée au CCB afin d'avoir une idée sur quels auraient pu être les raisons qui ont pu pousser à un tel retard et une accumulation aussi importante de question par les secteurs concernés par la directive. La réponse que nous avons eu indiquait simplement que cette question n'a été gérée par l'Etat que depuis très récemment et que cette culture de la gestion cyber n'a pas encore pu s'implémenter totalement dans le pays.

Nous l'avons déjà mentionné, les exigences de la directive impliquent toute une série de mesures de sécurité à mettre en place informatiquement afin de protéger les entités considérées comme OSE. De ce fait, il apparaît comme essentiel d'impliquer tout un ensemble d'experts techniques sur la question qui permettrait de pouvoir traduire les exigences de la directive et de soutenir les autorités compétentes (sectorielles ou CCB par exemple) afin de rendre la chose accessible pour des OSE n'ayant pas la possibilité d'investir des montants colossaux dans des

entreprises de consultance afin de sous-traiter la question. La question de l'expertise technique est donc un point important de la conformité NIS.

Tout d'abord, le professeur Legay nous explique :

« il y a des gens qui sont des juristes et qui pressentent faire de la cybersécurité dans toutes les régions de Belgique. Elles occultent totalement la partie technique et ça, ça nous ridiculise vis à vis des pays voisins. Et donc un des gros problèmes de la Belgique, c'est non seulement le morcellement en entité fédérée, mais aussi le fait qu'une administration trop juriste et non pas du tout pas du tout technique, a pris en main cette discipline. Ce qui nous ridiculise quand vous voyez que le CCB est principalement guidé par des juristes et que du côté de l'ANSSI en France, c'est géré par des techniciens. Regardons ce qui se passe aux États Unis, aux États Unis, les ingénieurs dominent clairement dans le domaine. Et donc tout shifter sur le juridique en Belgique n'est pas intelligent. Ça, c'est clairement un problème que nous avons. Alors je pense à contrario que tout mettre sur la technique n'est pas intelligent non plus. Mais nous sommes incapables de faire un bon mix [...] il y a de la mécompréhension et cette mécompréhension est entretenue par des gens qui ont pondus des cadres de lois dont ils ne comprennent pas l'applicabilité. Le simple fait que les entreprises disent mais moi pour fonctionner « je vais devoir bloquer ça (les exigences NIS) parce que si je le laisse arriver je ne fonctionnerai plus » et c'est ainsi que vous prenez un retard énorme. Vous perdez la collaboration d'acteurs parce que vous avez des braquages d'un côté comme de l'autre ».

Le CCB estime cependant que cette pluridisciplinarité existe déjà dans son organisation en précisant :

« la cybersécurité, ce n'est pas qu'une histoire de technicien. Je pense que la Commission européenne a essayé dans la mise en œuvre de s'appuyer au centre des connaissances des centres, etc. C'est comme ça que vont créer le réseau, générer justement un pôle vraiment technique, vraiment technique, sur la cybersécurité. Mais ce pôle technique doit s'appuyer aussi sur des décisions politiques stratégiques. Et ça, ce n'est

pas nécessairement ce n'est pas au technicien, à l'expert, à sa personnalité, à décider qu'est-ce qu'au niveau national pour nous faire ou comment, quelle est la priorité à donner à tel ou tel ? Ce n'est pas son rôle, donc il y a des rôles différents à attribuer. Et justement, je pense que la maturité dans le domaine, c'est justement de créer cette interdisciplinarité et d'avoir à la fois des experts, à la fois des informaticiens, des techniciens aussi, des responsables relations internationales, juridiques, communication nous travaillons ensemble, je coordonne et je pense que cet aspect-là a été pris en compte. Maintenant, dans certains cas, c'est vrai qu'il y a un dialogue à mettre en place et c'est très compliqué. ».

Cependant, afin de déterminer si cette vulgarisation des exigences de la directive NIS a bien eu lieu sur le terrain, nous avons posé la question à plusieurs OSE concernés dans des secteurs différents afin de déterminer la logique de ces acteurs et de pouvoir l'analyser. La directive ne donne pas de détails sur la manière concrète dont ses exigences doivent être implémentées. Les autorités nationales existent donc pour fournir ce soutien aux OSE afin de pouvoir traduire ces obligations en un langage unique et compréhensible pour tout le monde. Il en ressort que ce point n'a malheureusement pas été gérée efficacement. La loi elle-même se référant à des normes existantes :

« Finalement on s'appuyait pas mal sur le CCB je pense aussi pour la mise en place de notre SMS etc. mais il faut de l'expertise et pour ça le CCB n'a pas forcément l'expertise liée au secteur parce qu'il n'y a pas qu'une norme à respecter si on veut, mais disons qu'on veut respecter la loi et la norme ISO27001, on a des spécifications techniques, on a des normes industrielles par rapport aux chemins de fer. Et alors de nouveau, ça devient très sectoriel parce que, finalement, il faut tout respecter. ».

La même chose a été appliquée dans une OSE de distribution d'eau :

« En fait la directive NIS, c'est un ensemble de recommandations générales qu'il faut en bon père de famille mettre en place pour minimiser tous les risques d'intrusion, de piratage, de tout ce qui peut nuire à l'activité de distribution d'eau. Et donc ces recommandations, elles sont très, très vagues et donc nous nous sommes fait encadrer par une société

de consultance qui nous met un peu le pied à l'étrier pour nous dire d'aller plutôt vers la norme ISO 27001 ».

Tout d'abord, les ressources semblent manquer au niveau de l'autorité nationale qu'est le CCB. L'implication d'expertise technique est jugée insuffisante sur une matière aussi technique que la cybersécurité jugée même « *pilotée uniquement par des juristes* ». Le CCB n'a également pas la capacité de faire des retours à chacun des OSE qui se posent des questions sur l'application de la législation. De ce fait, un manque de ressources (capital humain) est constatable au sein du CCB.

2. L'efficacité bureaucratique

Un autre critère à prendre en considération est la capacité de légiférer par le gouvernement. La directive ayant été promulguée en 2016, le CCB nous précise dès lors que :

« le gouvernement était en affaires courantes et donc il fallait en plus faire passer ça en affaires courantes, ce qui fait quand on est en affaires courantes, on a beaucoup plus de difficultés d'obtenir des décisions, des choix politiques et que le gouvernement ne peut pas aller au-delà de ce qui est imposé juste par des obligations internationales. Ça limitait le champ d'application ou de possibilités. Donc ça, ça a compliqué pas mal la tâche. A l'époque la NVA et le ministre de l'Intérieur étaient NVA et c'est la NVA qui est la porte du gouvernement qui est partie aujourd'hui. Normalement, on devait piloter aussi avec le Premier ministre mais il a quitté la famille, donc il fallait attendre une réorganisation du gouvernement. Et tout ça a pris beaucoup de temps et en attendant, on ne savait pas travailler. On ne savait rien faire. ».

La prise de décision était dès lors difficile. Néanmoins, cet entretien a pu mettre en évidence un point important de la difficulté de transposition qui est la complexité des interactions entre les acteurs multiples existants au sein du territoire belge :

« Le principe, c'est que la compétence en matière de sécurité publique et qui comprend un petit peu la cybersécurité, est une compétence fédérale. Mais c'est une compétence résiduelle, c'est à dire que, parce qu'elle est attribuée à personne c'est le fédéral qui s'en occupe. Mais si sur certains aspects ou dans le futur, on disait que la cybersécurité complètement ou certaines parties est une compétence régionale, ça deviendrait régional,

communautaire. Donc il y a une question de compétence qui est un peu délicate à prendre en compte ».

En effet, la collaboration entre les niveaux de pouvoir en Belgique est un point central de la transposition de la directive NIS car un dialogue constant a dû être mis en place afin de pouvoir arriver à une ligne directrice claire sur le plan national.

Le professeur Legay nous confirme d'ailleurs ce point en précisant que :

« la difficulté, évidemment, c'est que ces trois lignes politiques ne collaborent que très peu et souvent au niveau administratif. Ce qui évidemment crée des frustrations puisque vous savez que la recherche et l'innovation sont très fortement régionalisées en Belgique. Et donc bien souvent en fait, ce qui se passe au Centre fédéré pour la CCB, c'est qu'une petite frustration des acteurs universitaires puisque le CCB, contrairement au CCB (ANSSI) français, ne les consulte pas. Donc il y a beaucoup de choses qui se mettent en place. Mais la coordination, on va dire interrégionale et avec l'État fédéral, reste pour moi trop centrée sur les administrations. Et je le crains en tout cas pour l'État fédéral, totalement déconnectée de la réalité du terrain. ».

Cette difficulté dans le dialogue est principalement due à l'implication aussi importante d'acteurs différents. En effet, la directive NIS devait être transposée dans la législation nationale. Mais comme précisé par le CCB, cette compétence n'était pas explicitement attribuée au fédéral. De ce fait, le fédéral est en charge de cette compétence résiduelle et a voulu impliquer les régions dans sa quête de transposition de la directive NIS. Le retard de transposition avait été soulevé lors de l'élaboration de la loi au Parlement, visibles dans les travaux parlementaires du 12 mars 2019 du projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique :

« À l'initiative du CCB et du Centre de crise, les représentants des administrations régionales ont été invités, au cours de l'année 2018, à différentes réunions de travail sur le projet de loi NIS. Les différentes versions du projet de loi ont ainsi été transmises aux services régionaux concernés. Le CCB et le Centre de crise ont répondu aux questions reçues des administrations régionales. Le projet de loi prévoit aussi la possibilité de créer des autorités sectorielles, composées de représentants de l'État fédéral, des Communautés et des Régions. ».

La Belgique a opté pour une gestion sectorielle de ses OSE. Ce système permet plusieurs choses, notamment d'avoir une connaissance des entités, du contexte sectoriel et des spécificités liées au secteur. Néanmoins, les secteurs confrontés à ces défis ont tout de même besoin d'un soutien technique que le CCB n'est pas toujours en mesure d'apporter aux entités concernées. Les travaux parlementaires du 12 mars 2019 du projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique permettent également de déceler un autre souci lié à ce gestion sectorielle de la conformité NIS. En effet, l'ancien Ministre de la Sécurité et de l'Intérieur Pieter de Crem précisait qu'il était envisagé de créer un Comité national de sécurité de la fourniture et de la distribution d'eau potable, lequel serait composé de représentants de l'État fédéral, de la Région wallonne, de la Région de Bruxelles-Capitale et de la Région flamande. Le secteur de l'eau est donc le seul secteur ne disposant pas de cet appui par une autorité sectorielle préexistante.

L'efficacité bureaucratique est donc également remise en question sur base de nos entretiens. En effet, la question de la compétence résiduelle de la cybersécurité implique que chacun des niveaux administratifs ne prend pas la responsabilité de prendre des décisions. Ceci est également visible pour le CCB qui ne veut pas prendre de décision et se contente d'un rôle consultatif. De ce fait, chaque administration se rejette la balle de la décision de l'application concrète des exigences de la directive NIS. Les travaux parlementaires du 12 mars 2019 du projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique permettent également de mettre en évidence le retard causé par l'implication de plusieurs niveaux de pouvoir (Région, services fédéraux, communautés, etc.). Le rôle de l'Union européenne peut également être remis en cause car la directive laisse le champ trop large aux Etats membres et permet des dérogations trop importantes. Ceci tend à réduire la compliance (Dimitrova & Steunenberg, 2000). Nous l'avons vu également, l'application et la gestion selon Tallberg peuvent conduire à de meilleurs résultats qu'un système ne se basant que sur l'un d'entre eux (2002). En l'espèce, nous avons pu constater un système imparfait basé sur le renforcement des capacités mais l'application de règles coercitives étant manquante. Aucune sanction n'a été pour l'instant prononcée pour non-respect de la directive NIS et le flou persiste encore l'éventuelle possibilité que cela puisse se produire dans un avenir proche. Les données obtenues permettent également de confirmer les résultats de l'étude de Falkner, Hartlapp, Leiber & Treib (2004) en mettant en avant les lacunes administratives et les problèmes d'interprétation.

3. L'autonomie domestique

L'identification des opérateurs de services essentiels est l'enjeu le plus important pour l'application de la directive NIS. Notre entretien avec le CCB (Centre pour la cybersécurité de Belgique) nous a révélé que la directive n'avait pas réussi à instaurer un système qui imposait une approche unique :

« [...] l'identification des opérateurs. Si je prends l'exemple du secteur de la santé il y a eu des grandes divergences. Par exemple aux Pays Bas ou en Belgique, il n'y a aucun opérateur qui a été identifié alors qu'à côté de ça, au Luxembourg ou en France ou même au Portugal, il y en a eu un certain nombre ».

La directive laissant libre la désignation des « OSE » (opérateurs de services essentiels), les secteurs impliqués sont fondamentalement différents d'un pays à l'autre. Ce point indique que les Etats membres ont des capacités d'implication et de résistance de secteurs très différents, et qu'en Belgique, ces secteurs ont été restreints au minimum afin de ne pas engendrer de coût superflu qui ne seraient pas supportables. Le CCB nous indiquait également :

« C'est la première fois en Belgique qu'il y avait une législation complexe sur la cybersécurité. Il n'y a jamais eu avant donc forcément, il fallait parler le même langage, expliquer ce qu'on essayait de faire, de mettre en œuvre. Et entre autres aussi, il y avait des discussions qui étaient un peu compliquées avec la santé. La preuve, eux ne voulaient pas que la directive NIS s'applique à leur secteur alors que c'était une obligation de directive. Mais finalement, ils ont discuté sur l'identification et ils n'ont pas pu identifier. Certains secteurs n'étaient pas volontaires, pas encouragés à participer ou ne voulait pas participer. ».

Nous remarquons que les secteurs potentiellement considérés comme OSE ont participé aux discussions de l'identification des OSE. Ces **discussions ont pu engendrer de blocages importants**, car une fois de plus, la directive NIS requiert des mesures de sécurité qui engendrent, notamment, des coûts importants à mettre en place.

Le professeur Legay va même plus loin dans son explication de cette délimitation des OSE :

« Disons que pour la directive NIS, on était tellement en retard dans l'implémentation que si on avait voulu à un moment où on a enfin pu la transcrire en loi, si on avait voulu impliquer tous les OSE comme les français, l'économie belge se serait écroulée. Donc on n'a pas eu le choix et c'est un peu le problème

qu'on va avoir avec NIS2 c'est l'Europe qui va décider et donc là on va se retrouver en difficulté. Il aurait probablement fallu en impliquer plus mais que d'un point de vue économique, ça aurait été une catastrophe, donc impossible à faire dû au retard pris ».

Enfin, l'autonomie domestique selon laquelle l'Etat peut prendre des décisions sans tenir compte des acteurs pouvant imposer un veto (« *veto players* »). Bien qu'aucun de ces « *veto players* » ne s'est mobilisé lors de la phase d'élaboration de la loi NIS, ceux-ci ont tout de même fait obstacle en n'appliquant pas les exigences de la directive ou en les appliquant de manière détournée. Dans le cas de la Belgique, les OSE et les FSN (fournisseurs de services numériques) ont ce pouvoir d'empêcher une compliance parfaite aux exigences de la directive NIS malgré qu'elles soient des acteurs de niveau inférieur (Steunenberg, 2006), notamment par le pouvoir d'appréciation qui leur est laissé par l'autorité nationale de déterminer la manière dont sera appliquée les exigences de la directive (qui sont rappelons le très vagues dans leur formulation).

4. Résultats

Cette analyse de notre première hypothèse nous a permis de montrer que le modèle PCP s'applique en partie mais la « Capacité » permet d'expliquer en grande partie le retard de la Belgique dans sa transposition et sa difficulté de mise en conformité.

En ce qui concerne le Pouvoir et la Politisation, ces points ne se retrouvent pas d'une manière explicite dans le cas présent. En effet, les débats de 2016 au Parlement européen n'indiquent pas d'opposition claire à l'élaboration de la directive NIS.

A cette époque, les partis politiques belges étaient représentés par les groupes suivants au Parlement :

Groupe (Parlement européen)	Parti politique belge membre
PPE	CD&V, Les engagés
ECR	NVA
ALDE	Open VLD, MR
S&D	PS, SPA
ENF (dissout depuis)	VB

Malgré la présence de ceux-ci lors des débats, nous n'avons pu déceler d'opposition importante

au projet de directive. Ce point sera néanmoins détaillé dans la partie traitant du processus de « *shaping* ».

L'objectif principal de la directive NIS reste une harmonisation des pratiques dans le marché commun européen. Cependant, on a pu voir que cette uniformisation est pour l'instant difficilement réalisable en pratique car rien qu'au sein de la Belgique, des différences notables peuvent être observées au sein d'un même secteur. Beaucoup de points ont été laissés à l'appréciation des administrations et celles-ci n'ont pas pu trancher ces points et se sont finalement retournés vers les OSE afin qu'ils déterminent eux-mêmes leurs obligations. Néanmoins, cette directive arrive dans un contexte tout à fait nouveau. La nouvelle directive (NIS2) va laisser moins de pouvoir d'appréciation aux Etats membres ce qui forcera une harmonisation plus importante.

C. Processus de « *shaping* » (façonnage)

Afin de poursuivre notre analyse, il est également important d'analyser la phase de « *shaping* » tel que développé par Börzel (2021) pour la directive NIS. Ce point, sera développé à deux niveaux concurrents tel que mentionné précédemment : le niveau domestique et le niveau européen.

1. Le niveau « domestique »

Börzel (2021) mentionne tout d'abord l'implication des « veto players ». Ces acteurs, agissant par intérêt propre (contraire à ceux décrits dans une norme), vont rendre la compliance à la directive moins coûteuse (orientation des résultats). Börzel (2021) émet deux conclusions :

- La politisation augmente les chances de « non-compliance » aux lois européennes coûteuses
- Les Etats membres qui affirment que des politiques européennes coûteuses vont devenir politisés vont avoir un avantage dans le façonnage et plus particulièrement dans des pays où un euroscepticisme important est observable.

Néanmoins, les deux points avancés par Börzel sont observables de manière indirecte dans le cadre de la directive NIS. Premièrement, nous avons pu voir qu'il y avait une politisation très faible concernant cette directive. Ces acteurs belges (entreprises, administrations, etc.) qui auraient pu jouer le rôle de veto n'ont pas exercé une pression suffisante que pour orienter les propos des délégations belges aux diverses instances qui ont pu participer au processus législatif de la directive NIS. Ceci n'est tout de fois pas vraie pour d'autres pays comme la France par sa député Marie-Christine Arnautu du groupe ENF qui militait par exemple pour une « *approche réglementaire contraignante plutôt que volontaire* ». Bien qu'il n'existe pas de preuve empirique pour ce point, il peut facilement être imaginé qu'un certain nombre de « veto players » français ne voulaient pas une approche réglementaire et donc qui supposerait un contrôle et des sanctions plus strictes. De cette façon, la compliance serait plus difficile contrairement à un système basé sur le « volontariat ».

Deuxièmement, l'absence d'un euroscepticisme en Belgique peut également expliquer son absence dans les efforts de façonnage de la directive NIS. La Belgique supporte fortement les politiques européennes (bien qu'elle ne soit pas toujours parmi les pays étant en mesure de transposer ces normes) ce qui vient décrédibiliser les chances d'avoir des « veto players » au niveau européen qui justifierait un façonnage pour la Belgique.

2. Le niveau européen

Börzel (2021) affirme qu'une plus grande politisation d'un sujet est étroitement lié au fait qu'elle suscite des débats ou non au parlement. Moins de participation ou de débat réduit donc la saillance d'une politique européenne. La compliance aux politiques européennes est plus coûteuse pour certains Etats membres comparé à d'autres. Ceci est donc principalement déterminé par leur capacité à façonner une norme afin de la faire correspondre aux préférences individuelles. Les politiques coûteuses n'engendrent cependant pas de facto de la non-compliance (Börzel, 2021).

Encore une fois, notre analyse se basera sur les éléments empiriques à notre disposition. Notre plus grande source de données pour le « *shaping* » au niveau européen réside dans les discussions au Parlement européen et au Conseil européen. Les députés et divers intervenants ont des positions qui méritent une attention particulière.

Premièrement, comme énoncé plus haut, les députés français ont beaucoup plaidé pour une approche moins contraignante pour les OSE et FSN concernés par la directive. En effet, le compte rendu *in extenso* des débats mercredi 6 juillet 2016 permet de voir que certains députés affichaient une volonté bien précise quant à la directive. La députée Dominique Bilde du groupe ENF précisait par exemple dans les débats que : « *ce texte mérite tout de même d'être approfondi, notamment dans son approche règlementaire plus contraignante que volontariste comportant des obligations de coopération avec des organes de la Commission européenne sous peine de sanctions, son nivellement par le bas pour certaines normes de sécurité afin de pallier les faiblesses législatives de certains pays, ou encore son insuffisance de protection personnelle face aux fournisseurs de services numériques.* ». Bien que cette étude ne soit pas comparative, nous pouvons voir comment une tentative de façonnage aurait pu avoir lieu pour réduire les coûts de compliance pour les entités concernées.

La position des députés belges ne marque pas de réelle volonté de façonner la directive d'une façon particulière. Aucune prise de position claire n'est visible durant les débats parlementaires. Ce point n'est cependant pas sans raison. Souvent, les délégations belges n'ont fait que suivre les avis des autres Etats membres.

Nous rappelons que le modèle PCP proposé par Börzel (2021) place la « Capacité » au centre du « *shaping* ». Pour les raisons que nous avons vues plus haut, ce qui a poussé à avoir des difficultés dans le « *taking* » de la directive ont indubitablement été alimenté par une incapacité

dans le « *shaping* » de la directive. Nous voyons donc l'interconnexion entre ces deux notions essentielles.

3. Résultats

Comme avancé dans notre deuxième hypothèse, l'absence de tentatives de « *shaping* » d'un Etat conduit à une compliance moins élevée. En effet, nous avons pu remarquer que la Belgique n'a pas tenté de façonner la directive afin de la faire correspondre à une réalité qui n'existait pas dans le pays. Des pays comme la France ont pu néanmoins aboutir à des situations favorables comme précisé par Philippe Latombe (membre du groupe Mouvement Démocrate et apparentés) lors de la Séance du mercredi 31 janvier 2018 de l'Assemblée nationale : « *Le Gouvernement a fait le choix de ne pas reprendre cette liste dans le présent texte pour permettre d'étendre la qualification d'opérateurs de services essentiels à de nouveaux domaines en fonction du contexte et des nouvelles menaces qui pourraient apparaître. Cette souplesse répond d'ailleurs à une demande de l'ANSSI – l'Agence nationale de la sécurité des systèmes d'information.* ». Il n'est pas étonnant de pouvoir constater la différence dans la compliance qui sépare nos deux pays voisins.

Selon la théorie de Börzel (2021) certains Etats disposeraient d'un pouvoir de veto important par rapport au poids qu'ils ont grâce à leur participation financière (« big three » composé de l'Allemagne, France et Italie) au niveau du Conseil européen. Cependant, nous n'avons pas constaté de blocage pour cette directive. Le vote sur la directive au Conseil européen était d'ailleurs unanime.

Ce façonnage n'a cependant pas uniquement lieu à travers les votes des Etats membres. Certains pays disposant de moins de capacités de veto ou de contributions budgétaires peuvent également orienter la décision des instances européennes à travers des expertises offertes à la Commission européenne (Börzel, 2021). La capacité des Etats à utiliser correctement leur ressource à disposition leur permettent d'avoir une position de force plus importante que leur poids relatif au sein de l'Union (Panke, 2010). Nous n'avons constaté aucune expertise de la Belgique à ce niveau cependant.

Nous l'avons mentionné dans les résultats sur le « *taking* » : la Belgique n'était pas prête à faire face aux coûts imposés par la directive. Ceci est soutenu par les divers témoignages récoltés sur le terrain affirmant l'incapacité du CCB à faire face aux nouveaux défis dans tous les secteurs concernés. Cependant, cette « non-compliance » a été encore plus accentuée par l'absence de façonnage visant à réduire les coûts de « compliance ».

D. Conclusions

Ces éléments nous permettent également d'affirmer la théorie Falkner, Hartlapp & Treib (2007) sur la typologie des mondes de la compliance en inscrivant la Belgique dans le « World of transposition neglect ». Les critères de Falkner, Hartlapp & Treib pour catégoriser un pays sont tous remplis :

- **Le processus de transposition était retardé et superficiel** (la Belgique étant un des derniers pays à transposer la directive et la législation de transposition laissant trop de libertés aux OSE)
- **L'échec bureaucratique** (l'implication trop importante de niveaux de pouvoir qui complique le dialogue entre acteurs de terrain et pouvoirs décisionnels ainsi que le refus de prendre la compétence pour chacun des niveaux de pouvoir impliqués).

Dans une étude menée par Börzel, Hofmann & Panke (2012), une tendance de la Belgique à ne pas respecter les obligations du droit européen avait été avancée par les auteurs. Ceci ne fait que soutenir la catégorisation ci-dessus. Cette tendance est également renforcée par les variables de performance propre à la Belgique constaté par Bursens (2002), également applicables ici : le contexte constitutionnel et administratif (l'attribution non explicite de la compétence de cybersécurité à un niveau de pouvoir), la capacité institutionnelle (l'incapacité du CCB d'effectuer une gestion optimale de la question), la pression d'adaptation administrative et juridique (de par le contexte cyber dans sa globalité et l'accroissement des menaces), la communication et la continuité.

Le modèle PCP nous permet de dégager les causes de ce retard et d'affirmer en partie l'hypothèse formulée au début de ce mémoire. En effet, la capacité de la Belgique est remise en question par toute une série d'indicateurs (ressources, efficacité bureaucratique, autonomie domestique).

Enfin pour reprendre les conclusions du modèle de Börzel, nous avons essayé d'établir un comparatif de ceux-ci pour leur application à la directive NIS :

Conclusions de Börzel	Réponse en fonction des données obtenues
Les États puissants ayant une faible capacité et un faible niveau de politisation affichent plus de non-conformité que les États membres moins puissants, dotés d'une forte capacité et une forte propension à la politisation.	L'hypothèse semble se vérifier ici car la Belgique affiche une capacité et politisation faible ainsi qu'une non-conformité.
Plus les institutions limitent le pouvoir de façonnage des États, rendent la résistance au respect plus coûteuse pour eux, préservent ou renforcent leur capacité à faire face aux coûts de mise en conformité et réduisent les risques de politisation des coûts de mise en conformité, moins le risque de non-conformité est élevé.	Cette conclusion peut s'observer indirectement dans le cadre de la directive NIS. L'Etat belge n'ayant pas rendue la non-conformité coûteuse, le risque de non-conformité n'en a été que plus élevé.
Les secteurs politiques qui imposent des coûts plus élevés, étant plus susceptibles d'être politisés, attirent plus de non-conformité que les secteurs politiques qui sont moins exigeants pour la capacité de l'État et sont politiquement moins sensibles.	Le secteur implique des coûts potentiellement élevés par les risques liés à la cybersécurité. Les coûts réels potentiellement engendrés par la directive peuvent conduire à la non-conformité observée. En effet, la directive nécessite des moyens humains, financiers, d'expertise et de contrôle importants.
Plus les États sont intégrés dans le droit communautaire, plus ils sont conformes.	Cette hypothèse se vérifie par les études précédentes réalisées (voir supra). La Belgique se conforme d'une façon ou d'une autre aux règles communautaires.

Moins l'UE et le droit communautaire sont légitimes, plus le risque de non-conformité est élevé.	L'hypothèse est difficilement observable ici. La Belgique ne s'est jamais caractérisée par un eurosceptisme particulier. Cependant, ce secteur a généré beaucoup de non-conformité.
--	---

Des lacunes législatives peuvent également être relevées ce qui renforce encore plus ce sentiment de « non-capacité » de la Belgique de traiter un sujet aussi contemporain que la cybersécurité avec efficacité. Nous avons pu voir à travers les entretiens que les incitations (positives ou négatives) étaient absentes du processus de l'implémentation de la directive NIS. En effet, à part une menace fantôme de sanction qui ne s'est jamais concrétisée, les OSE avaient peu de raison de traiter ce chantier en priorité. Ceci confirme également l'étude de Batory (2012). Néanmoins, la gestion de l'Union européenne peut également être remise en question au même titre (absence de sanctions). Ceci confirme également l'étude de König & Mäder (2013) car les chances de succès immédiats de la directive NIS1 succès étaient faibles et les coûts de sanction élevés. Il est également intéressant de noter comment l'ambition initiale de la Belgique en matière de gouvernance de cybersécurité a finalement été tempérée par son application sur le terrain (Steunenberg, 2007).

E. Discussion et limites de la recherche

Notre analyse nous a permis d'identifier plusieurs points de convergence avec la théorie existante. Toutefois, comme chaque étude, celle-ci dispose de limites. En tant qu'étudiants, il est important pour nous de pouvoir constater les limites de notre propre travail afin d'ouvrir la voie à un approfondissement du sujet. Notre étude n'a pas, et ne peut pas, avoir prétention de trouver une réponse définitive à un phénomène aussi complexe que celui étudié. Selon nous, c'est là que réside toute la base d'un travail scientifique : en analysant un sujet et en identifiant où des erreurs ont pu être commises et les rectifier afin d'arriver à des conclusions plus précises.

Tout d'abord, cette étude isolée du cas de la Belgique ne permet pas de tirer des conclusions plus générales sur le plan européen. N'ayant pas orienté les recherches vers une étude comparative, il est difficile de comparer ces résultats à d'autres qui auraient pu être observables en Europe. C'est pourquoi, bien que cette analyse nous fournisse des éléments de réponse importants, il serait intéressant de pouvoir la poursuivre afin de comprendre si ces deux notions de « *shaping* » et « *taking* » de Börzel s'appliquent réellement de manière fondamentalement différente selon les contextes des autres pays. Encore une fois, nous avons dû limiter notre analyse afin de ne pas nous engager dans une étude interminable aux fins de ce mémoire. Ceci constitue néanmoins une base importante, et le sujet mérite d'être approfondi, notamment en analysant ces deux mêmes notions à travers la nouvelle directive NIS2. Il est tout à fait possible, que les Etats ayant pris conscience de l'ampleur du chantier avec la directive NIS1 soient engagés dans un effort de « *shaping* » plus important. Tout comme l'étude réalisée par Angelova, Dannwolf & König (2012) sur l'efficacité administrative et la préférence politique des acteurs, des résultats ambigus peuvent être observés dans le cas présent. L'échantillon devrait être plus important afin d'arriver à des conclusions suscitant moins d'ambiguïté.

Deuxièmement, un sujet impliquant aussi fortement des aspects aussi techniques que la cybersécurité peut vite porter à confusion. Ce point, bien que pouvant sembler anodin, peut vite déstabiliser la recherche en essayant de mêler ces aspects techniques aux théories de Sciences politiques. Il faut, comme pour tout travail d'analyse dans notre domaine, prendre du recul par rapport à ceci et analyser un sujet dans sa globalité.

Finalement, le terrain joue un facteur très important dans l'analyse de ce sujet. En effet, il est parfois difficile de pouvoir d'obtenir des entretiens avec des personnes pouvant répondre à nos interrogations. Manque de temps, peur de mettre son organisation dans l'embarras, etc. jouent tous un rôle important.

Il est clair que l'analyse ne devrait pas s'arrêter ici, des éléments importants ont pu être dégagés de cette première étude du sujet et d'autres analyses sous d'autres angles permettraient de faire ressortir de nouvelles informations pertinentes.

Bibliographie

Articles

Angelova, M., Dannwolf, T. & König, T. (2012, octobre). How Robust Are Compliance Findings ? A Research Synthesis. *Journal of European Public Policy*, 19(8), 1269-1291. <https://doi.org/10.1080/13501763.2012.705051>

Batory, A. (2012, 25 janvier). Why do anti-corruption laws fail in Central Eastern Europe ? A target compliance perspective. *Regulation & Governance*, 6(1), 66-82. <https://doi.org/10.1111/j.1748-5991.2011.01125.x>

Bergström, C. F., Farrell, H. & Héritier, A. (2007, mars). Legislate or delegate ? Bargaining over implementation and legislative authority in the EU. *West European Politics*, 30(2), 338-366. <https://doi.org/10.1080/01402380701239814>

Börzel, T. (2010, mars). European Governance : Negotiation and Competition in the Shadow of Hierarchy. *JCMS : Journal of Common Market Studies*, 48(2), 191-219. <https://doi.org/10.1111/j.1468-5965.2009.02049.x>

Börzel, T. A. & Risse, T. (2017). From the euro to the Schengen crises : European integration theories, politicization, and identity politics. *Journal of European Public Policy*, 25(1), 83-108. <https://doi.org/10.1080/13501763.2017.1310281>

Börzel, T. A. (2005, avril). Mind the gap ! European integration between level and scope. *Journal of European Public Policy*, 12(2), 217-236. <https://doi.org/10.1080/13501760500043860>

Börzel, T. A., Hofmann, T. & Panke, D. (2012, mai). Caving in or sitting it out ? Longitudinal patterns of non-compliance in the European Union. *Journal of European Public Policy*, 19(4), 454-471. <https://doi.org/10.1080/13501763.2011.607338>

Börzel, T. A., Hofmann, T., Panke, D. & Sprungk, C. (2010, 27 juillet). Obstinate and Inefficient : Why Member States Do Not Comply With European Law. *Comparative Political Studies*, 43(11), 1363-1390. <https://doi.org/10.1177/0010414010376910>

Bursens, P. (2002). Why Denmark and Belgium Have Different Implementation Records : On Transposition Laggards and Leaders in the EU. *Scandinavian Political Studies*, 25(2), 173-195. <https://doi.org/10.1111/1467-9477.00068>

Checkel, J. T. (2001). Why Comply ? Social Learning and European Identity Change. *International Organization*, 55(3), 553-588. <https://doi.org/10.1162/00208180152507551>

Christoph Knill & Jale Tosun. (2009). Post-accession transposition of EU law in the new member states : a cross-country comparison*. *European integration online papers (EIoP)*, 13(2), 1. <https://doi.org/10.1695/2009018>

Dimitrova, A. & Steunenberg, B. (2000). The Search for Convergence of National Policies in the European Union. *European Union Politics*, 1(2), 201-226. <https://doi.org/10.1177/1465116500001002003>

Duina, F. (1997). Explaining Legal Implementation in the European Union. *International Journal of the Sociology of Law*, 25(2), 155-179. <https://doi.org/10.1006/ijsl.1997.0039>

Falkner, G. & Treib, O. (2008, mars). Three Worlds of Compliance or Four ? The EU-15 Compared to New Member States. *JCMS : Journal of Common Market Studies*, 46(2), 293-313. <https://doi.org/10.1111/j.1468-5965.2007.00777.x>

Falkner, G. (2010). Institutional Performance and Compliance with EU Law : Czech Republic, Hungary, Slovakia and Slovenia. *Journal of Public Policy*, 30(1), 101-116. <https://doi.org/10.1017/s0143814x09990183>

Falkner, G., Hartlapp, M. & Treib, O. (2007, mai). Worlds of compliance : Why leading approaches to European Union implementation are only sometimes-true theories ? *European Journal of Political Research*, 46(3), 395-416. <https://doi.org/10.1111/j.1475-6765.2007.00703.x>

Falkner, G., Hartlapp, M., Leiber, S. & Treib, O. (2004). Non-Compliance with EU Directives in the Member States : Opposition through the Backdoor ? *West European Politics*, 27(3), 452-473. <https://doi.org/10.1080/0140238042000228095>

Haverland, M., Steunenberg, B. & Van Waarden, F. (2010). Sectors at Different Speeds : Analysing Transposition Deficits in the European Union*. *JCMS : Journal of Common Market Studies*, 49(2), 265-291. <https://doi.org/10.1111/j.1468-5965.2010.02120.x>

Huelshoff, M. G., Sperling, J. & Hess, M. (2005). Is Germany a 'good European' ? German compliance with EU Law. *German Politics*, 14(3), 354-370. <https://doi.org/10.1080/09644000500268845>

König, T. & Luetgert, B. (2009). Troubles with Transposition ? Explaining Trends in Member-State Notification and the Delayed Transposition of EU Directives. *British Journal of Political Science*, 39(1), 163-194. <https://doi.org/10.1017/s0007123408000380>

König, T., & Mäder, L. (2012). Non-conformable, partial and conformable transposition: A competing risk analysis of the transposition process of directives in the EU15. *European Union Politics*, 14(1), 46–69. <https://doi.org/10.1177/1465116512447703>

König, T., & Mäder, L. (2013). The Strategic Nature of Compliance: An Empirical Evaluation of Law Implementation in the Central Monitoring System of the European Union. *American Journal of Political Science*, 58(1), 246–263. doi:10.1111/ajps.12038

Maglaras, L., Drivas, G., Noou, K., & Rallis, S. (2018). NIS directive : The case of Greece. *EAI Endorsed Transactions on Security and Safety*, 4(14), 154769. <https://doi.org/10.4108/eai.15-5-2018.154769>

Mathias, G. (2018). NIS : Vers un cadre harmonisé pour la cybersécurité ? *Sécurité globale*, 15(3), 25. <https://doi.org/10.3917/secug.183.0025>

Hartlapp, M., & Falkner, G. (2009). Problems of operationalization and data in EU compliance research. *European Union Politics*, 10(2), 281-304. <https://doi.org/10.1177/1465116509103370>

Panke, D. (2010). Small states in the European Union : structural disadvantages in EU policy-making and counter-strategies. *Journal of European Public Policy*, 17(6), 799-817. <https://doi.org/10.1080/13501763.2010.486980>

Quémener, M. (2016). La directive NIS, un texte majeur en matière de cybersécurité. *Sécurité et stratégie*, 23, 50-56. <https://doi.org/10.3917/sestr.023.0050>

Sprungk, C. (2011). How Policy-Shaping Might (Not) Affect Policy-Taking: The Case Of National Parliaments in the European Union. *Journal of European Integration*, 33(3), 323–340. doi:10.1080/07036337.2010.546843

Steunenberg, B. (2006). Turning Swift Policy-making into Deadlock and Delay. *European Union Politics*, 7(3), 293–319. doi:10.1177/1465116506066258

Steunenberg, B. (2007). A policy solution to the European Union's transposition puzzle: Interaction of interests in different domestic arenas. *West European Politics*, 30(1), 23–49. doi:10.1080/01402380601019639

Steunenberg, B. (2010). Is big brother watching? Commission oversight of the national implementation of EU directives. *European Union Politics*, 11(3), 359–380. doi:10.1177/1465116510369395

Steunenberg, B., & Rhinard, M. (2010). The transposition of European law in EU member states: between process and politics. *European Political Science Review*, 2(03), 495–520. doi:10.1017/s1755773910000196

Steunenberg, B., & Toshkov, D. (2009). Comparing transposition in the 27 member states of the EU: the impact of discretion and legal fit. *Journal of European Public Policy*, 16(7), 951–970. doi:10.1080/13501760903226625

Tallberg, J. (2002). Paths to Compliance : Enforcement, Management, and the European Union. *International Organization*, 56(3), 609-643. <https://doi.org/10.1162/002081802760199908>

Thomson, R., Torenvlied, R., & Arregui, J. (2007). The Paradox of Compliance: Infringements and Delays in Transposing European Union Directives. *British Journal of Political Science*, 37(04). doi:10.1017/s0007123407000373

Toshkov, D. (2007). In search of the worlds of compliance: culture and transposition performance in the European Union. *Journal of European Public Policy*, 14(6), 933–959. doi:10.1080/13501760701497956

Zhelyazkova, A., & Yordanova, N. (2015). Signalling “compliance”: The link between notified EU directive implementation and infringement cases. *European Union Politics*, 16(3), 408–428. doi:10.1177/1465116515576394

Ouvrages

Börzel, T. A. (2021). *Why Noncompliance : The Politics of Law in the European Union*. Amsterdam University Press.

Van Campenhoudt, L., Marquet, J., Quivy, R. (2017). *Manuel de recherche en sciences sociales*. Dunod.

Sites Internet

ANSIP (s.d.). *Estonia isn't perfect enough to teach other countries tech* (s. d.). Retrieved from <https://www.eastr-asso.org/content/ansip-estonia-isn-t-perfect-enough-teach-other-countries-tech-source-euractivcom>

Centre for Cyber security Belgium (2023). *The NIS 2 Directive : What does it mean for my organization ?* Retrieved from <https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization>

Centre pour la Cybersécurité Belgique (2021). *Une cyberstratégie 2.0 pour propulser la Belgique au rang des pays les moins vulnérables d'Europe*. Retrieved from <https://ccb.belgium.be/fr/actualit%C3%A9/une-cyberstrat%C3%A9gie-20-pour-propulser-la-belgique-au-rang-des-pays-les-moins-vuln%C3%A9rables-d>

Centre pour la Cybersécurité Belgique (2022). *3e anniversaire de la Loi nationale transposant la « Directive NIS »*. Retrieved from <https://ccb.belgium.be/fr/actualit%C3%A9/3e-anniversaire-de-la-loi-nationale-transposant-la-%C2%AB-directive-nis-%C2%BB>

Centre pour la Cybersécurité Belgique (2023). *Secteurs vitaux*. Retrieved from <https://ccb.belgium.be/fr/secteurs-vitaux>

Centre pour la Cybersécurité de Belgique (2023). *Organisation*. Retrieved from <https://ccb.belgium.be/fr/organisation>

Claude, G. (2021a). Méthodes inductives et déductives : définition, méthodologie et exemples. *Scribbr*. Retrieved from <https://www.scribbr.fr/methodologie/methodes-inductives-deductives/>

Commission Européenne (s. d.). *Groupe de coopération SRI*. Retrieved from <https://digital-strategy.ec.europa.eu/fr/policies/nis-cooperation-group>

Cyber Security Coalition (2021). *Our mission is to fight against cybercrime*. Retrieved from <https://www.cybersecuritycoalition.be/about/>

Cyberlegis (2021). *NIS Directive In Germany - Implementation & Specificities*, 2021), Retrieved from https://cyberlegis.legal/wp-content/uploads/2021/03/NIS-Directive-in-Germany_Cyberlegis_Flyer_2021.pdf

DigitalEurope (2021). *NIS Implementation Tracker*. Retrieved from <https://www.digitaleurope.org/resources/nis-implementation-tracker/>

ENISA (s.d.). *Information Sharing and Analysis Centers (ISACs)*. Retrieved from <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing>

ENISA (s.d.). *NIS Directive Tool*. Retrieved from <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/nis-visualtool>

EUR-LEX (2016). *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des*

réseaux et des systèmes d'information dans l'Union. Retrieved from <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L1148>

EUR-LEX (2016). *Proposition de Directive Du Parlement Européen Et Du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union.* Retrieved from <https://eur-lex.europa.eu/legal-content/FR/HIS/?uri=CELEX:32016L1148>

International Bar Association (s. d.). *Implementing the EU's NIS directive in Romania.* Retrieved from <https://www.ibanet.org/article/578803AA-EECB-437D-BB35-7CB3D75E80BD>

ISACS (2021). *Empowering EU-ISACs.* Retrieved from <https://www.isacs.eu/>

Législations

Loi du 07/04/2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (M.B 03/05/2019)

